PATENT
8008-1048

IN THE U.S. PATENT AND TRADEMARK OFFICE

In re application of:	Mao MASUHIRO et al.
	Conf.:
Appl. No.:	NEW NON-PROVISIONAL
	Group:
Filed:	December 8, 2003
	Examiner:
Title:	MAINTENANCE INTERFACE USER AUTHENTICATION METHOD AND APPARATUS IN CLIENT/SERVER TYPE DISTRIBUTION SYSTEM

CLAIM TO PRIORITY

Assistant Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

December 8, 2003

Sir:

Applicant(s) herewith claim(s) the benefit of the priority filing date of the following application(s) for the above-entitled U.S. application under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55:

Country	Application No.	Filed
JAPAN	2002-356839	December 9, 2002

Certified copy(ies) of the above-noted application(s) is(are) attached hereto.

Respectfully submitted,

YOUNG & THOMPSON

Benoit Castel

Benoit Castel, Reg. No. 35,041

745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297

BC/ma

Attachment(s): 1 Certified Copy(ies)

US

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年１２月 ９日

出 願 番 号
Application Number: 特願２００２－３５６８３９

[ST. 10/C]: [ＪＰ２００２－３５６８３９]

出 願 人
Applicant(s): 日本電気株式会社

２００３年１０月２９日

特許庁長官
Commissioner,
Japan Patent Office 今 井 康 夫

出証番号 出証特２００３－３０８９５１６

【書類名】　特許願
【整理番号】　41810247
【提出日】　平成14年12月 9日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 11/30
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　益弘　麻央
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　渡辺　康弘
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100088959
　【弁理士】
　【氏名又は名称】　境　廣巳
【手数料の表示】
　【予納台帳番号】　009715
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9002136
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　クライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法および装置

【特許請求の範囲】

【請求項１】　複数のクライアント装置とサーバ装置とがネットワークを通じて接続されたクライアント・サーバ型分散システムにおいて、前記サーバ装置は、サーバ側コンソールから、利用者認証情報と前記クライアント装置の指定とを含む利用者認証情報設定要求、および前記クライアント装置の指定を含む利用者認証情報設定無効要求を受け付ける要求受付手段と、前記要求受付手段で受け付けられた前記利用者認証情報設定要求および前記利用者認証情報設定無効要求を指定された前記クライアント装置に前記ネットワークを通じて転送する要求転送手段とを備え、前記それぞれのクライアント装置は、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段と、前記サーバ装置から前記ネットワークを通じて前記利用者認証情報設定要求を受信したときに前記利用者認証情報設定要求に含まれる利用者認証情報を前記利用者認証手段に設定し、前記サーバ装置から前記ネットワークを通じて前記利用者認証情報設定無効要求を受信したときに前記利用者認証手段に設定されている利用者認証情報を無効にするリモート要求処理手段とを備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項２】　請求項１記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記それぞれのクライアント装置における前記利用者認証手段への利用者認証情報の設定は、前記サーバ側コンソールからのみ設定可能としたことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項３】　請求項１または２記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記サーバ装置は、前記要求転送手段が転送する利用者認証情報設定要求中の利用者認証情報を暗号化する暗号化手段を備え、前記それぞれのクライアント装置に、前記リモート要求処理手段が受信した利用者認証情報設定要求中の暗号化された利用者認証情報を

復号化する復号化手段を備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項４】　請求項１または２記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記それぞれのクライアント装置は、前記利用者認証手段に既に設定されている利用者認証情報が前記ネットワークを通じて受信した新たな利用者認証情報設定要求によって再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする強制切断手段を備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項５】　請求項１または２記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段を備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項６】　請求項５記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長する利用時間延長手段を備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項７】　請求項６記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記利用時間延長手段は、前記保守インタフェースを開放してから初回のログイン要求があった際に、前記利用時間管理手段で管理されている残り利用時間が予め定められた一定時間以内かどうかを判定し、一定時間以内であれば予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長するものであることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項８】　請求項６記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記利用時間延長手段は、前記保守インタフェースを開放してからの初回のログイン中、前記利用時間管理手段で管理されている残り利用時間が予め定められた一定時間以内となったかどうかを判定し、一定時間以内になった場合に予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長するものであることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項９】　請求項５または６記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記利用時間管理手段は、前記利用可能時間として前記サーバ装置から送信された前記利用者認証情報設定要求で指定された利用可能時間を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項１０】　請求項５または６記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記利用時間管理手段は、前記利用可能時間として前記クライアント装置に予め記憶されている利用可能時間基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項１１】　請求項５または６記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記利用時間管理手段は、前記利用可能時間として、前記サーバ装置から送信された前記利用者認証情報設定要求で利用可能時間が指定されているときは該指定された利用可能時間を使用し、指定されていないときは前記クライアント装置に予め記憶されている利用可能時間基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項１２】　請求項１または２記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している

利用者の利用を強制的に不可能にするログイン回数管理手段を備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項１３】　請求項１２記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記ログイン回数管理手段は、前記ログイン可能回数として前記サーバ装置から送信された前記利用者認証情報設定要求で指定されたログイン可能回数を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項１４】　請求項１３記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記ログイン回数管理手段は、前記ログイン可能回数として前記クライアント装置に予め記憶されているログイン可能回数基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項１５】　請求項１３記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記ログイン回数管理手段は、前記ログイン可能回数として、前記サーバ装置から送信された前記利用者認証情報設定要求でログイン可能回数が指定されているときは該指定されたログイン可能回数を使用し、指定されていないときは前記クライアント装置に予め記憶されているログイン可能回数基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項１６】　請求項１または２記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にする認証無効化手段を備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項１７】　ａ）サーバ装置が、サーバ側コンソールから、利用者認証情報とクライアント装置の指定とを含む利用者認証情報設定要求を受け付け、指定された前記クライアント装置にネットワークを通じて転送するステップと、

ｂ）前記クライアント装置が、前記ネットワークを通じて前記利用者認証情報設定要求を受信し、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段に設定するステップと、

ｃ）前記サーバ装置が、前記サーバ側コンソールから、前記クライアント装置の指定を含む利用者認証情報設定無効要求を受け付け、指定された前記クライアント装置に前記ネットワークを通じて転送するステップと、

ｄ）前記クライアント装置が、前記ネットワークを通じて前記利用者認証情報設定無効要求を受信し、前記利用者認証手段に設定されている利用者認証情報を無効にするステップと、

を含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項１８】　請求項１７記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記それぞれのクライアント装置における前記利用者認証手段への利用者認証情報の設定は、前記サーバ側コンソールからのみ設定可能としたことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項１９】　請求項１７または１８記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップａは、前記サーバ装置が前記転送する利用者認証情報を暗号化する処理を含み、前記ステップｂは、前記クライアント装置が前記受信した利用者認証情報を復号化する処理を含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項２０】　請求項１７または１８記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップｂは、前記利用者認証手段に既に設定されている利用者認証情報が前記受信した新たな利用者認証情報に再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする処理を含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項２１】　請求項１７または１８記載のクライアント・サーバ型分散

システムにおける保守インタフェース利用者認証方法において、

ｅ）それぞれの前記クライアント装置が、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするステップを含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項２２】　請求項２１記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、

ｆ）それぞれの前記クライアント装置が、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用可能時間を延長するステップを含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項２３】　請求項２２記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記スナップｆは、前記保守インタフェースを開放してから初回のログイン要求があった際に、前記ステップｅで管理されている残り利用時間が予め定められた一定時間以内かどうかを判定し、一定時間以内であれば予め定められた延長時間だけ前記残り利用時間を延長することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項２４】　請求項２２記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップｆは、前記保守インタフェースを開放してからの初回のログイン中、前記ステップｅで管理されている残り利用時間が予め定められた一定時間以内となったかどうかを判定し、一定時間以内になった場合に予め定められた延長時間だけ前記残り利用時間を延長することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項２５】　請求項２１または２２記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップｅ

における前記利用可能時間として前記サーバ装置から送信された前記利用者認証情報設定要求で指定された利用可能時間を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項２６】　請求項２１または２２記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップｅにおける前記利用可能時間として前記クライアント装置に予め記憶されている利用可能時間基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項２７】　請求項２１または２２記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップｅにおける前記利用可能時間として、前記サーバ装置から送信された前記利用者認証情報設定要求で利用可能時間が指定されているときは該指定された利用可能時間を使用し、指定されていないときは前記クライアント装置に予め記憶されている利用可能時間基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項２８】　請求項１７または１８記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、
ｅ）それぞれの前記クライアント装置が、前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするステップを含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項２９】　請求項２８記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップｅにおける前記ログイン可能回数として前記サーバ装置から送信された前記利用者認証情報設定要求で指定されたログイン可能回数を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項３０】　請求項２９記載のクライアント・サーバ型分散システムに

おける保守インタフェース利用者認証方法において、前記ステップｅにおける前記ログイン可能回数として前記クライアント装置に予め記憶されているログイン可能回数基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項３１】　請求項２９記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップｅにおける前記ログイン可能回数として、前記サーバ装置から送信された前記利用者認証情報設定要求でログイン可能回数が指定されているときは該指定されたログイン可能回数を使用し、指定されていないときは前記クライアント装置に予め記憶されているログイン可能回数基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項３２】　請求項１７または１８記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、
ｅ）それぞれの前記クライアント装置が、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にするステップを含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項３３】　複数のクライアント装置とネットワークを通じて接続されるサーバ装置において、サーバ側コンソールから、前記クライアント装置が保守インタフェースの利用に際して利用者の認証を行う利用者認証手段に設定する利用者認証情報と前記クライアント装置の指定とを含む利用者認証情報設定要求、および前記クライアント装置の指定を含む利用者認証情報設定無効要求を受け付ける要求受付手段と、前記要求受付手段で受け付けられた前記利用者認証情報設定要求および前記利用者認証情報設定無効要求を指定された前記クライアント装置に前記ネットワークを通じて転送する要求転送手段とを備えることを特徴とするサーバ装置。

【請求項３４】　請求項３３記載のサーバ装置において、前記要求転送部が転送する利用者認証情報設定要求中の利用者認証情報を暗号化する暗号化手段を備えることを特徴とするサーバ装置。

【請求項３５】　請求項３３記載のサーバ装置において、それぞれの前記クライアント装置が前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段に設定する前記利用可能時間を、前記利用者認証情報設定要求に含めて送信する構成を備えることを特徴とするサーバ装置。

【請求項３６】　請求項３３記載のサーバ装置において、それぞれの前記クライアント装置が前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段に設定する前記ログイン可能回数を、前記利用者認証情報設定要求に含めて送信する構成を備えることを特徴とするサーバ装置。

【請求項３７】　サーバ装置にネットワークを通じて接続されるクライアント装置において、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段と、利用者認証情報を含む利用者認証情報設定要求を前記ネットワークを通じて前記サーバ装置から受信したときに前記利用者認証情報設定要求に含まれる利用者認証情報を前記利用者認証手段に設定し、利用者認証情報設定無効要求を前記ネットワークを通じて前記サーバ装置から受信したときに前記利用者認証手段に設定されている利用者認証情報を無効にするリモート要求処理手段を備えることを特徴とするクライアント装置。

【請求項３８】　請求項３７記載のクライアント装置において、前記利用者認証手段への利用者認証情報の設定は、前記サーバ装置から受信した利用者認証情報設定要求のみにより可能としたことを特徴とするクライアント装置。

【請求項３９】　請求項３７または３８記載のクライアント装置において、前記サーバ装置から前記ネットワークを通じて受信した前記利用者認証情報設定要求中の暗号化された利用者認証情報を復号化する復号化手段を備えることを特徴とするクライアント装置。

【請求項４０】　請求項３７または３８記載のクライアント装置において、前記利用者認証手段に既に設定されている利用者認証情報が前記ネットワークを通じて受信した新たな利用者認証情報設定要求によって再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする強制切断手段を備えることを特徴とするクライアント装置。

【請求項４１】　請求項３７または３８記載のクライアント装置において、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段を備えることを特徴とするクライアント装置。

【請求項４２】　請求項４１記載のクライアント装置において、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長する利用時間延長手段を備えることを特徴とするクライアント装置。

【請求項４３】　請求項３７または３８記載のクライアント装置において、前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段を備えることを特徴とするクライアント装置。

【請求項４４】　請求項３７または３８記載のクライアント装置において、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にする認証無効化手段を備えることを特徴とするクライアント装置。

【請求項４５】　複数のクライアント装置とネットワークを通じて接続されるサーバ装置を構成するコンピュータを、サーバ側コンソールから、前記クライアント装置が保守インタフェースの利用に際して利用者の認証を行う利用者認証手段に設定する利用者認証情報と前記クライアント装置の指定とを含む利用者認証情報設定要求、および前記クライアント装置の指定を含む利用者認証情報設定

無効要求を受け付ける要求受付手段、前記要求受付手段で受け付けられた前記利用者認証情報設定要求および前記利用者認証情報設定無効要求を指定された前記クライアント装置に前記ネットワークを通じて転送する要求転送手段、として機能させることを特徴とするサーバプログラム。

【請求項４６】　請求項４５記載のサーバプログラムにおいて、前記コンピュータを、更に、前記要求転送手段が転送する利用者認証情報設定要求中の利用者認証情報を暗号化する暗号化手段として機能させるサーバプログラム。

【請求項４７】　請求項４５記載のサーバプログラムにおいて、前記要求受付手段および前記要求転送手段は、それぞれの前記クライアント装置が前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段に設定する前記利用可能時間を、前記サーバ側コンソールから受け付けて前記利用者認証情報設定要求に含めて転送することを特徴とするサーバプログラム。

【請求項４８】　請求項４５記載のサーバプログラムにおいて、前記要求受付手段および前記要求転送手段は、それぞれの前記クライアント装置が前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段に設定する前記ログイン可能回数を、前記サーバ側コンソールから受け付けて前記利用者認証情報設定要求に含めて転送することを特徴とするサーバプログラム。

【請求項４９】　サーバ装置にネットワークを通じて接続されるクライアント装置を構成するコンピュータを、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段、利用者認証情報を含む利用者認証情報設定要求を前記ネットワークを通じて前記サーバ装置から受信したときに前記利用者認証情報設定要求に含まれる利用者認証情報を前記利用者認証手段に設定し、利用者認証情報設定無効要求を前記ネットワークを通じて前記サーバ装置から受信したとき

に前記利用者認証手段に設定されている利用者認証情報を無効にするリモート要求処理手段、として機能させることを特徴とするクライアントプログラム。

【請求項５０】　請求項４９記載のクライアントプログラムにおいて、前記利用者認証手段への利用者認証情報の設定は、前記サーバ装置から受信した利用者認証情報設定要求のみにより可能としたことを特徴とするクライアントプログラム。

【請求項５１】　請求項４９または５０記載のクライアントプログラムにおいて、前記コンピュータを、更に、前記サーバ装置から前記ネットワークを通じて受信した前記利用者認証情報設定要求中の暗号化された利用者認証情報を復号化する復号化手段として機能させることを特徴とするクライアントプログラム。

【請求項５２】　請求項４９または５０記載のクライアントプログラムにおいて、前記コンピュータを更に、前記利用者認証手段に既に設定されている利用者認証情報が前記ネットワークを通じて受信した新たな利用者認証情報設定要求によって再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする強制切断手段として機能させることを特徴とするクライアントプログラム。

【請求項５３】　請求項４９または５０記載のクライアントプログラムにおいて、前記コンピュータを更に、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段として機能させることを特徴とするクライアントプログラム。

【請求項５４】　請求項５３記載のクライアントプログラムにおいて、前記コンピュータを更に、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長する利用時間延長手段として機能させることを特徴とするクライアントプログラム。

【請求項５５】　請求項４９または５０記載のクライアントプログラムにおいて、前記コンピュータを更に、前記利用者認証手段に利用者認証情報が設定さ

れてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段として機能させることを特徴とするクライアントプログラム。

【請求項５６】　請求項４９または５０記載のクライアントプログラムにおいて、前記コンピュータを更に、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にする認証無効化手段として機能させることを特徴とするクライアントプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はクライアント・サーバ型分散システムにおけるクライアント装置の保守インタフェース利用者認証方法及び装置に関し、特にクライアント装置に設けられた保守インタフェースの利用に際して利用者の認証を行うための利用者認証情報を、ネットワークを通じてサーバ装置から設定でき、また無効化できる保守インタフェース利用者認証方法及び装置に関する。

【０００２】

【従来の技術】

クライアント・サーバ型分散システムにおいては、各クライアント装置が地理的に分散して設置されているため、運用時にはＬＡＮを介してＬＡＮ上の遠隔保守コンソールから各クライアント装置の遠隔保守を行うことがある。しかしながら、ＬＡＮ上からの遠隔保守であるためセキュリティの確保が必要であり、この対策としてクライアント装置の保守インタフェースを予め設定された利用者認証情報を知るものだけが利用できるようにしている。具体的には、クライアント装置に接続されたローカル保守コンソールを用いて、クライアント装置にユーザ名およびパスワードで構成される利用者認証情報を事前に設定しておき、遠隔保守コンソールからログイン、ログアウトと呼ばれる一般的な操作が行われる際に認証用のユーザ名およびパスワードを入力させ、クライアント装置側で登録されてい

るユーザ名およびパスワードとの一致が確認された場合に限り、遠隔保守コンソールからの保守作業を可能としている。

【０００３】

このように、或る装置の保守を遠隔保守コンソールからネットワークを介して実施する場合に、ユーザ名とパスワードを用いた利用者認証を行うようにした技術は後述する特許文献１に記載されている。但し、特許文献１には、ユーザ名およびパスワードを事前に登録する具体的な方法は開示されていない。また、後述する特許文献２には、インターネットに端末型ダイアルアップ接続された複数の端末と単一の保守サーバとの間で、ＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃの認証鍵を共有するための端末－保守サーバ間認証鍵共有方法が記載されているが、設定した認証鍵を無効にして保守インタフェースを閉塞する点については記載されていない。

【０００４】

【特許文献１】

特許第３２１４４２３号

【特許文献２】

特開２００１－１９７０５８号公報

【０００５】

【発明が解決しようとする課題】

ネットワーク上からの遠隔保守のセキュリティを確保するために、上述したようにクライアント装置の保守インタフェースを利用する際には認証情報による利用者認証を実施しているが、事前に設定したユーザ名およびパスワードが漏洩すると、ネットワーク上に接続する他の端末から同様な手順でユーザ名・パスワードが入力されればクライアント装置へアクセス可能となり、保守インタフェースを介してハッキング等の被害にあう可能性がある。システムの運用中にこのようなハッキング等の被害を受ける危険性が生じた場合、クライアント装置に登録されたユーザ名・パスワードを消去したり、別のユーザ名およびパスワードに書き換えることで防御する必要があるが、地理的に分散した各々のクライアント装置の設置場所に出向いてそのローカル保守コンソールから認証情報の消去や変更を行

うのは、手間と時間がかかる上、クライアント側のローカル保守コンソールが既に取り払われていた場合には再接続する手間もかかってしまうという課題がある。また、認証情報を一旦削除してしまうと、運用中における遠隔保守コンソールからの保守ができないため、保守を行う際にはクライアント装置の設置場所に再び出向いて認証情報を設定しなければならない煩わしさもある。つまり、従来のクライアント・サーバ型システムの保守インタフェース利用者認証方式では、セキュリティの確保と保守の容易性を両立するのが困難であった。

【０００６】

そこで、本発明の目的は、クライアント装置における保守インタフェースのセキュリティを確保でき、サーバ装置側から複数のクライアント装置の保守インタフェース利用許可／禁止を管理可能なクライアント・サーバ型システムの保守インタフェース利用者認証方法および装置を提供することにある。

【０００７】

また、本発明の他の目的は、クライアント装置の保守インタフェースの利用可能時間を管理することで、長時間にわたりクライアント装置の保守インタフェースが開放され続けることによるハッキング等の機会を最小化することが可能なクライアント・サーバ型システムの保守インタフェース利用者認証方法および装置を提供することにある。

【０００８】

さらに、本発明の別の目的は、クライアント装置の保守インタフェースの利用可能時間の延長や保守者からの保守インタフェースの閉塞を可能にすることにより、保守インタフェースの利便性を高めたクライアント・サーバ型システムの保守インタフェース利用者認証方法および装置を提供することにある。

【０００９】

【課題を解決するための手段】

本発明の第１のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、複数のクライアント装置とサーバ装置とがネットワークを通じて接続されたクライアント・サーバ型分散システムにおいて、前記サーバ装置は、サーバ側コンソールから、利用者認証情報と前記クライアント装置の指定

とを含む利用者認証情報設定要求、および前記クライアント装置の指定を含む利用者認証情報設定無効要求を受け付ける要求受付手段と、前記要求受付手段で受け付けられた前記利用者認証情報設定要求および前記利用者認証情報設定無効要求を指定された前記クライアント装置に前記ネットワークを通じて転送する要求転送手段とを備え、前記それぞれのクライアント装置は、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段と、前記サーバ装置から前記ネットワークを通じて前記利用者認証情報設定要求を受信したときに前記利用者認証情報設定要求に含まれる利用者認証情報を前記利用者認証手段に設定し、前記サーバ装置から前記ネットワークを通じて前記利用者認証情報設定無効要求を受信したときに前記利用者認証手段に設定されている利用者認証情報を無効にするリモート要求処理手段とを備える。

【００１０】

この第１のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置にあっては、複数のクライアント装置の保守インタフェースに対するセキュリティ確保のための利用者認証情報をネットワーク経由でサーバ側コンソールから遠隔で設定でき、また既に設定されている利用者認証情報をネットワーク経由でサーバ側コンソールから遠隔で無効化することができ、個々のクライアント装置の保守インタフェースに対するセキュリティ管理をサーバ側で一括管理することができる。

【００１１】

本発明の第２のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、第１のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記それぞれのクライアント装置における前記利用者認証手段への利用者認証情報の設定は、前記サーバ側コンソールからのみ設定可能とする。これにより、個々のクライアント装置の保守インタフェースがサーバ側コンソールからのみ開放でき、より一層セキュリティを確保することができる。

【００１２】

本発明の第３のクライアント・サーバ型分散システムにおける保守インタフェー

ス利用者認証装置は、第１または第２のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記サーバ装置は、前記要求転送手段が転送する利用者認証情報設定要求中の利用者認証情報を暗号化する暗号化手段を備え、前記それぞれのクライアント装置に、前記リモート要求処理手段が受信した利用者認証情報設定要求中の暗号化された利用者認証情報を復号化する復号化手段を備える。これにより、クライアント装置の保守インタフェースを開放するための利用者認証情報のネットワークからの漏洩が防止でき、セキュリティを確保することができる。

【００１３】

本発明の第４のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、第１または第２のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記それぞれのクライアント装置は、前記利用者認証手段に既に設定されている利用者認証情報が前記ネットワークを通じて受信した新たな利用者認証情報設定要求によって再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする強制切断手段を備える。これにより、クライアント装置の保守インタフェースを通じて悪意のアクセスが行われている場合に、サーバ側コンソールからの遠隔制御によって、そのアクセスを直ちに停止させることができると同時に侵入に使った利用者認識情報を無効化し、且つ正規の保守のために新たな利用者認証情報を再設定することができる。

【００１４】

本発明の第５のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、第１または第２のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段を備える。これにより、それぞれのクライアント装置の保守インタフェースが長時間にわたって開放され続け、悪意のアクセス

の危険性が高くなるのを防止することができる。

【００１５】

本発明の第６のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、第５のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長する利用時間延長手段を備える。具体的には、前記利用時間延長手段は、前記保守インタフェースを開放してから初回のログイン要求があった際に、前記利用時間管理手段で管理されている残り利用時間が予め定められた一定時間以内かどうかを判定し、一定時間以内であれば予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長する。また、前記利用時間延長手段は、前記保守インタフェースを開放してからの初回のログイン中、前記利用時間管理手段で管理されている残り利用時間が予め定められた一定時間以内となったかどうかを判定し、一定時間以内になった場合に予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長するものであっても良い。これにより、クライアント装置の保守インタフェースを開放してから実際に保守者がクライアント装置の保守インタフェースを利用するまでに暫く時間がかかり、残り利用時間が短い時点でログインしても充分な保守作業を行うことができ、しかも初回のログインだけ延長を認めるのでセキュリティを確保することができる。

【００１６】

ここで、第５または第６のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記利用時間管理手段は、前記利用可能時間として、前記サーバ装置から送信された前記利用者認証情報設定要求で指定された利用可能時間を使用するようにしても良いし、前記クライアント装置に予め記憶されている利用可能時間基準値を使用するようにしても良い。また、前記サーバ装置から送信された前記利用者認証情報設定要求で利用可能時間が指定されているときは該指定された利用可能時間を使用し、指定されていないときは前記クライアント装置に予め記憶されている利用可能時間基準値を使用するように

しても良い。

【００１７】

本発明の第７のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、第１または第２のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段を備える。これにより、ログイン、ログアウトを何度も繰り返す悪意の利用者に対するセキュリティを確保することができる。

【００１８】

ここで、第７のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記ログイン回数管理手段は、前記ログイン可能回数として、前記サーバ装置から送信された前記利用者認証情報設定要求で指定されたログイン可能回数を使用するようにしても良いし、前記クライアント装置に予め記憶されているログイン可能回数基準値を使用するようにしても良い。また、前記サーバ装置から送信された前記利用者認証情報設定要求でログイン可能回数が指定されているときは該指定されたログイン可能回数を使用し、指定されていないときは前記クライアント装置に予め記憶されているログイン可能回数基準値を使用するようにしても良い。

【００１９】

本発明の第８のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、第１または第２のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にする認証無効化手段を備える。これにより、保守作業の終了と同時に保守インタフェースを閉塞でき、クライアント装置の保守インタフェースのセキュリティを確保

することができる。

【００２０】

本発明の第１のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、ａ）サーバ装置が、サーバ側コンソールから、利用者認証情報とクライアント装置の指定とを含む利用者認証情報設定要求を受け付け、指定された前記クライアント装置にネットワークを通じて転送するステップと、ｂ）前記クライアント装置が、前記ネットワークを通じて前記利用者認証情報設定要求を受信し、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段に設定するステップと、ｃ）前記サーバ装置が、前記サーバ側コンソールから、前記クライアント装置の指定を含む利用者認証情報設定無効要求を受け付け、指定された前記クライアント装置に前記ネットワークを通じて転送するステップと、ｄ）前記クライアント装置が、前記ネットワークを通じて前記利用者認証情報設定無効要求を受信し、前記利用者認証手段に設定されている利用者認証情報を無効にするステップとを含んで構成される。

【００２１】

この第１のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法にあっては、複数のクライアント装置の保守インタフェースに対するセキュリティ確保のための利用者認証情報をネットワーク経由でサーバ側コンソールから遠隔で設定でき、また既に設定されている利用者認証情報をネットワーク経由でサーバ側コンソールから遠隔で無効化することができ、個々のクライアント装置の保守インタフェースに対するセキュリティ管理をサーバ側で一括管理することができる。

【００２２】

本発明の第２のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第１のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記それぞれのクライアント装置における前記利用者認証手段への利用者認証情報の設定は、前記サーバ側コンソールからのみ設定可能とされる。これにより、個々のクライアント装置の保守インタフェースがサーバ側コンソールからのみ開放でき、より一層セキュリティを確保

することができる。

【００２３】

本発明の第３のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第１または第２のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップａは、前記サーバ装置が前記転送する利用者認証情報を暗号化する処理を含み、前記ステップｂは、前記クライアント装置が前記受信した利用者認証情報を復号化する処理を含んで構成される。これにより、クライアント装置の保守インタフェースを開放するための利用者認証情報のネットワークからの漏洩が防止でき、セキュリティを確保することができる。

【００２４】

本発明の第４のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第１または第２のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップｂは、前記利用者認証手段に既に設定されている利用者認証情報が前記受信した新たな利用者認証情報に再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする処理を含んで構成される。これにより、クライアント装置の保守インタフェースを通じて悪意のアクセスが行われている場合に、サーバ側コンソールからの遠隔制御によって、そのアクセスを直ちに停止させることができると同時に侵入に使った利用者認識情報を無効化し、且つ正規の保守のために新たな利用者認証情報を再設定することができる。

【００２５】

本発明の第５のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第１または第２のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、ｅ）それぞれの前記クライアント装置が、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするステップを含んで構成される。これにより、それぞれのクラ

イアント装置の保守インタフェースが長時間にわたって開放され続け、悪意のアクセスの危険性が高くなるのを防止することができる。

【００２６】

本発明の第６のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第５のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、ｆ）それぞれの前記クライアント装置が、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用可能時間を延長するステップを含んで構成される。具体的には、前記保守インタフェースを開放してから初回のログイン要求があった際に、前記ステップｅで管理されている残り利用時間が予め定められた一定時間以内かどうかを判定し、一定時間以内であれば予め定められた延長時間だけ前記残り利用時間を延長する。また、前記保守インタフェースを開放してからの初回のログイン中、前記ステップｅで管理されている残り利用時間が予め定められた一定時間以内となったかどうかを判定し、一定時間以内になった場合に予め定められた延長時間だけ前記残り利用時間を延長するようにしても良い。これにより、クライアント装置の保守インタフェースを開放してから実際に保守者がクライアント装置の保守インタフェースを利用するまでに暫く時間がかかり、残り利用時間が短い時点でログインしても充分な保守作業を行うことができ、しかも初回のログインだけ延長を認めるのでセキュリティを確保することができる。

【００２７】

ここで、第５および第６のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップｅにおける前記利用可能時間として、前記サーバ装置から送信された前記利用者認証情報設定要求で指定された利用可能時間を使用するようにしても良いし、前記クライアント装置に予め記憶されている利用可能時間基準値を使用するようにしても良い。また、前記サーバ装置から送信された前記利用者認証情報設定要求で利用可能時間が指定されているときは該指定された利用可能時間を使用し、指定されていないときは前記クライアント装置に予め記憶されている利用可能時間基準値を使用するようにしても良い。

【００２８】

本発明の第７のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第１または第２のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、ｅ）それぞれの前記クライアント装置が、前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするステップを含んで構成される。これにより、ログイン、ログアウトを何度も繰り返す悪意の利用者に対するセキュリティを確保することができる。

【００２９】

ここで、第７のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップｅにおける前記ログイン可能回数として、前記サーバ装置から送信された前記利用者認証情報設定要求で指定されたログイン可能回数を使用するようにしても良いし、前記クライアント装置に予め記憶されているログイン可能回数基準値を使用するようにしても良い。また、前記サーバ装置から送信された前記利用者認証情報設定要求でログイン可能回数が指定されているときは該指定されたログイン可能回数を使用し、指定されていないときは前記クライアント装置に予め記憶されているログイン可能回数基準値を使用するようにしても良い。

【００３０】

本発明の第８のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第１または第２のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、ｅ）それぞれの前記クライアント装置が、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にするステップを含んで構成される。これにより、保守作業の終了と同時に保守インタフェースを閉塞でき、クライアント装置の保守インタフェースのセキュリティを確保することができる。

【００３１】

本発明の第１のサーバ装置は、複数のクライアント装置とネットワークを通じて接続されるサーバ装置において、サーバ側コンソールから、前記クライアント装置が保守インタフェースの利用に際して利用者の認証を行う利用者認証手段に設定する利用者認証情報と前記クライアント装置の指定とを含む利用者認証情報設定要求、および前記クライアント装置の指定を含む利用者認証情報設定無効要求を受け付ける要求受付手段と、前記要求受付手段で受け付けられた前記利用者認証情報設定要求および前記利用者認証情報設定無効要求を指定された前記クライアント装置に前記ネットワークを通じて転送する要求転送手段とを備える。

【００３２】

この第１のサーバ装置にあっては、複数のクライアント装置の保守インタフェースに対するセキュリティ確保のための利用者認証情報をネットワーク経由でサーバ側コンソールから遠隔で設定でき、また既に設定されている利用者認証情報をネットワーク経由でサーバ側コンソールから遠隔で無効化することができ、個々のクライアント装置の保守インタフェースに対するセキュリティ管理をサーバ側で一括管理することができる。

【００３３】

本発明の第２のサーバ装置は、第１のサーバ装置において、前記要求転送部が転送する利用者認証情報設定要求中の利用者認証情報を暗号化する暗号化手段を備える。これにより、クライアント装置の保守インタフェースを開放するための利用者認証情報のネットワークからの漏洩が防止でき、セキュリティを確保することができる。

【００３４】

本発明の第３のサーバ装置は、第１のサーバ装置において、それぞれの前記クライアント装置が前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段に設定する前記利用可能時間を、前記利用者認証情報設定要求に含めて送信する構成を備える。これにより、それぞれのクラ

イアント装置の保守インタフェースが長時間にわたって開放され続け悪意のアクセスの危険性が高くなるのを防止するために使用する利用可能時間を、サーバ装置から遠隔でそれぞれのクライアント装置に設定することができる。

【００３５】

本発明の第４のサーバ装置は、第１のサーバ装置において、それぞれの前記クライアント装置が前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段に設定する前記ログイン可能回数を、前記利用者認証情報設定要求に含めて送信する構成を備える。これにより、ログイン、ログアウトを何度も繰り返す悪意の利用者に対するセキュリティを確保するためのログイン可能回数を、サーバ装置から遠隔で設定することができる。

【００３６】

本発明の第１のクライアント装置は、サーバ装置にネットワークを通じて接続されるクライアント装置において、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段と、利用者認証情報を含む利用者認証情報設定要求を前記ネットワークを通じて前記サーバ装置から受信したときに前記利用者認証情報設定要求に含まれる利用者認証情報を前記利用者認証手段に設定し、利用者認証情報設定無効要求を前記ネットワークを通じて前記サーバ装置から受信したときに前記利用者認証手段に設定されている利用者認証情報を無効にするリモート要求処理手段を備える。

【００３７】

この第１のクライアント装置にあっては、保守インタフェースに対するセキュリティ確保のための利用者認証情報をネットワーク経由でサーバ装置から遠隔で設定でき、また既に設定されている利用者認証情報をネットワーク経由でサーバ装置から遠隔で無効化することができ、クライアント装置の保守インタフェースに対するセキュリティ管理をサーバ側で管理することができる。

【００３８】

本発明の第２のクライアント装置は、第１のクライアント装置において、前記利用者認証手段への利用者認証情報の設定は、前記サーバ装置から受信した利用者認証情報設定要求のみにより可能とした構成を有する。これにより、クライアント装置の保守インタフェースがサーバ装置からのみ開放でき、より一層セキュリティを確保することができる。

【００３９】

本発明の第３のクライアント装置は、第１または第２のクライアント装置において、前記サーバ装置から前記ネットワークを通じて受信した前記利用者認証情報設定要求中の暗号化された利用者認証情報を復号化する復号化手段を備える。これにより、クライアント装置の保守インタフェースを開放するための利用者認証情報のネットワークからの漏洩が防止でき、セキュリティを確保することができる。

【００４０】

本発明の第４のクライアント装置は、第１または第２のクライアント装置において、前記利用者認証手段に既に設定されている利用者認証情報が前記ネットワークを通じて受信した新たな利用者認証情報設定要求によって再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする強制切断手段を備える。これにより、クライアント装置の保守インタフェースを通じて悪意のアクセスが行われている場合に、サーバ装置からの遠隔制御によって、そのアクセスを直ちに停止させることができると同時に侵入に使った利用者認識情報を無効化し、且つ正規の保守のために新たな利用者認証情報を再設定することができる。

【００４１】

本発明の第５のクライアント装置は、第１または第２のクライアント装置において、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段を備える。これにより、クライアント装置の保守インタフェースが長時間にわたって開放され続け、悪意のアクセスの危険性が高くな

るのを防止することができる。

【００４２】

本発明の第６のクライアント装置は、第５のクライアント装置において、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長する利用時間延長手段を備える。これにより、クライアント装置の保守インタフェースを開放してから実際に保守者がクライアント装置の保守インタフェースを利用するまでに暫く時間がかかり、残り利用時間が短い時点でログインしても充分な保守作業を行うことができ、しかも初回のログインだけ延長を認めるのでセキュリティを確保することができる。

【００４３】

本発明の第７のクライアント装置は、第１または第２のクライアント装置において、前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段を備える。これにより、ログイン、ログアウトを何度も繰り返す悪意の利用者に対するセキュリティを確保することができる。

【００４４】

本発明の第８のクライアント装置は、第１または第２のクライアント装置において、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にする認証無効化手段を備える。これにより、保守作業の終了と同時に保守インタフェースを閉塞でき、クライアント装置の保守インタフェースのセキュリティを確保することができる。

【００４５】

【発明の実施の形態】

次に本発明の実施の形態について図面を参照して詳細に説明する。

【００４６】

【発明の第１の実施の形態】

図１を参照すると、本発明の第１の実施の形態にかかるクライアント・サーバ型システムは、サーバ装置１と複数のクライアント装置３と遠隔保守コンソール５とがＬＡＮ６を通じて相互に通信可能に接続されている。また、サーバ装置１にはシリアルインタフェース等を通じてローカル保守コンソール２が接続されており、クライアント装置３にはシリアルインタフェース等を通じてローカル保守コンソール４が接続されている。以下、サーバ装置１に接続されたローカル保守コンソールをサーバ側ローカル保守コンソールと呼び、クライアント装置３に接続されたローカル保守コンソールをクライアント側ローカル保守コンソールと呼ぶ。クライアント側ローカル保守コンソール４は、クライアント装置３のシステムデータの設定や変更などを行うためにクライアント装置３の工事期間等に臨時に設置されるもので、運用中には接続しておかなくとも良い。これに対してサーバ側ローカル保守コンソール２は、サーバ装置３の障害や処理能力の監視、システムデータの設定や変更などを行うもので、運用中は必要時に接続される。例えば本発明をＶｏＩＰシステムであるクライアント・サーバ型ＩＰ－ＰＢＸに適用する場合、サーバ装置１は、ＩＰ－ＰＢＸにおいて呼制御を行うＭＧＣ（Ｍｅｄｉａ　Ｇａｔｅｗａｙ　Ｃｏｎｔｒｏｌｅｒ）に相当し、サーバ側ローカル保守コンソール２はＭＧＣに接続されたコンソールに相当する。また、クライアント装置３は、公衆電話網等との接続を行うＭＧ（Ｍｅｄｉａ　Ｇａｔｅｗａｙ）や電話機を収容するＭＣ（Ｍｅｄｉａ　Ｃｏｎｖｅｒｔｅｒ）あるいはＩＰ電話機に相当し、ローカル保守コンソール４はそれらに接続されたコンソールに相当する。なお、本発明はクライアント・サーバ型ＩＰ－ＰＢＸにのみ適用が限定されないのは勿論のことである。

【００４７】

サーバ装置１は、サーバ側ローカル保守コンソール２からクライアント装置３を指定した利用者認証情報設定要求および利用者認証情報設定無効要求を受け付ける要求受付部１１と、この要求受付部１１で受け付けられた要求をＬＡＮ６を通じて指定されたクライアント装置３に転送する要求転送部１２とを含んで構成される。

【００４８】

図２はサーバ側ローカル保守コンソール２から利用者認証情報設定要求が入力された際のサーバ装置１の処理例を示すフローチャートである。システム管理者等が、利用者認証情報の設定対象となるクライアント装置３の指定情報（例えばクライアント装置を一意に識別するクライアント装置名など）と、設定したい利用者認証情報としてのユーザ名およびパスワードとを含む利用者認証情報設定要求をサーバ側ローカル保守コンソール２から入力すると、この要求を要求受付部１１により受信し（Ｓ１０１）、同じく要求受付部１１によりユーザ名およびパスワードの桁数などの正常性をチェックする（Ｓ１０２）。桁数などが所定の条件を満足しない場合、要求は拒否される。問題がなければ、受け付けた利用者認証情報設定要求を要求受付部１１から要求転送部１２へ伝達する（Ｓ１０３）。次に、要求転送部１２により、利用者認証情報設定要求中で指定されているクライアント装置３のＩＰアドレスを、例えばクライアント装置名とＩＰアドレスの対応表（図示せず）などを参照して確認し（Ｓ１０４）、このＩＰアドレスを用いて利用者認証情報設定要求中のユーザ名およびパスワードを含む利用者認証情報設定指示をＬＡＮ６経由で対象クライアント装置３へ送信する（Ｓ１０５）。そして、対象クライアント装置３から利用者認証情報設定完了通知が返されてくると、この通知を要求転送部１２で受信して（Ｓ１０６）、要求受付部１１に伝達し（Ｓ１０７）、要求受付部１１がサーバ側ローカル保守コンソール２に利用者認証情報設定完了通知を出力する（Ｓ１０８）。

【００４９】

図３はサーバ側ローカル保守コンソール２から利用者認証情報設定無効要求が入力された際のサーバ装置１の処理例を示すフローチャートである。システム管理者等が、利用者認証情報の設定を無効にしたいクライアント装置３を指定した利用者認証情報設定無効要求をサーバ側ローカル保守コンソール２から入力すると、この要求を要求受付部１１により受信し（Ｓ１１１）、受信した利用者認証情報設定無効要求を要求受付部１１から要求転送部１２へ伝達する（Ｓ１１２）。次に、要求転送部１２により、利用者認証情報設定無効要求中で指定されているクライアント装置３のＩＰアドレスを確認し（Ｓ１１３）、このＩＰアドレスを

用いて利用者認証情報設定無効指示をＬＡＮ６経由で対象クライアント装置３へ送信する（Ｓ１１４）。そして、対象クライアント装置３から利用者認証情報設定無効完了通知が返されてくると、この通知を要求転送部１２で受信して（Ｓ１１５）、要求受付部１１に伝達し（Ｓ１１６）、要求受付部１１がサーバ側ローカル保守コンソール２に利用者認証情報設定無効完了通知を出力する（Ｓ１１７）。

【００５０】

他方、各々のクライアント装置３は、Ｔｅｌｎｅｔインタフェースに代表される保守インタフェース３０を有しており、また、保守対象となる保守対象部３１と、保守対象部３４の保守を行う利用者に対して認証情報に基づく利用者認証を行う利用者認証部３２と、ＬＡＮ６を通じてサーバ装置１から送られてくる利用者認証情報設定要求および利用者認証情報設定無効要求を受信し、各要求に応じた処理を実行するリモート要求処理部３３と、クライアント側ローカル保守コンソール４から入力される利用者認証情報設定要求および利用者認証情報設定無効要求を受信し、各要求に応じた処理を実行するローカル要求処理部３４と、遠隔保守コンソール５などＬＡＮ６上の装置からクライアント装置３へのログインおよびログアウトにかかる処理を実行するログイン・ログアウト処理部３５とを含んで構成される。保守対象部３１は、例えば、クライアント装置３を構成するハードウェアおよびソフトウェアの動作状況および障害状況ならびに各種のシステム設定データを記録するメモリ、ソフトウェアそのものなどである。また、保守対象部３１の保守とは、前記メモリに記憶された動作状況および障害状況の参照や、システム設定データおよびソフトウェアの変更などの操作である。

【００５１】

図４はサーバ装置１から利用者認証情報設定指示がＬＡＮ６経由で送信されてきた際のクライアント装置３の処理例を示すフローチャートである。ＬＡＮ経由で利用者認証情報設定指示が送信されてきたクライアント装置３は、この指示をリモート要求処理部３３で受信し（Ｓ１２１）、指示中のユーザ名およびパスワードが所定の桁数を満たすかどうかのチェックを行う（Ｓ１２２）。所定の条件を満たさない場合、この指示は拒否される。問題がなければ、この指示がリモート

要求処理部３３から利用者認証部３２に伝達される（Ｓ１２３）。利用者認識部３２は伝達された指示中のユーザ名およびパスワードを内部に記憶する（Ｓ１２４）。他方、リモート要求処理部３３は、要求元のサーバ装置３に対してＬＡＮ６経由で利用者認証情報設定完了通知を送信する（Ｓ１２５）。

【００５２】

図５はサーバ装置１から利用者認証情報設定無効指示がＬＡＮ６経由で送信されてきた際のクライアント装置３の処理例を示すフローチャートである。ＬＡＮ経由で利用者認証情報設定無効指示が送信されてきたクライアント装置３は、この指示をリモート要求処理部３３で受信し（Ｓ１３１）、利用者認証部３２に伝達する（Ｓ１３２）。利用者認識部３２は、内部に登録されているユーザ名およびパスワードを消去するなどして無効化する（Ｓ１３３）。他方、リモート要求処理部３３は、要求元のサーバ装置３に対してＬＡＮ６経由で利用者認証情報設定無効完了通知を送信する（Ｓ１３４）。

【００５３】

図６はクライアント側ローカル保守コンソール４から利用者認証情報設定要求が入力された際のクライアント装置３の処理例を示すフローチャートである。保守作業者等が、設定したい利用者認証情報としてのユーザ名およびパスワードを含む利用者認証情報設定要求をクライアント側ローカル保守コンソール４から入力すると、この要求をローカル要求処理部３４により受信し（Ｓ１４１）、同じくローカル要求処理部３４により、要求中のユーザ名およびパスワードが所定の桁数を満たすかどうかのチェックを行う（Ｓ１４２）。所定の条件を満たさない場合、この要求は拒否される。問題がなければ、要求中のユーザ名およびパスワードを含む利用者認証情報設定指示がローカル要求処理部３４から利用者認証部３２に伝達される（Ｓ１４３）。利用者認識部３２は伝達された指示中のユーザ名およびパスワードを内部に記憶する（Ｓ１４４）。他方、ローカル要求処理部３４は、利用者認証情報設定完了通知をクライアント側ローカル保守コンソール４へ出力する（Ｓ１４５）。

【００５４】

図７はクライアント側ローカル保守コンソール４から利用者認証情報設定無効要

求が入力された際のクライアント装置３の処理例を示すフローチャートである。保守作業者等が、設定されている利用者認証情報を無効化する利用者認証情報設定無効要求をクライアント側ローカル保守コンソール４から入力すると、この要求をローカル要求処理部３４により受信し（Ｓ１５１）、利用者認証部３２に伝達する（Ｓ１５２）。利用者認識部３２は、内部に登録されているユーザ名およびパスワードを消去するなどして無効化する（Ｓ１５３）。他方、ローカル要求処理部３４は、利用者認証情報設定無効完了通知をクライアント側ローカル保守コンソール４へ出力する（Ｓ１５４）。

【００５５】

図８は遠隔保守コンソール５からユーザ名およびパスワードの指定を含むログイン要求がＬＡＮ６経由で送信されてきた際のクライアント装置３の処理例を示すフローチャートである。ＬＡＮ経由でログイン要求が送信されてきたクライアント装置３は、このログイン要求をログイン・ログアウト処理部３５で受信し（Ｓ１６１）、ログイン要求中のユーザ名およびパスワードが所定の桁数等を満たすかどうかのチェックを行う（Ｓ１６２）。所定の条件を満たさない場合、このログイン要求は拒否される。問題がなければ、このログイン要求中のユーザ名およびパスワードを指定した認証指示がログイン・ログアウト処理部３５から利用者認証部３２に伝達される（Ｓ１６３）。利用者認識部３２は、内部の利用者認証情報が事前に登録されているかどうかを判定し（Ｓ１６４）、登録されていれば（Ｓ１６５でＹＥＳ）、ログイン・ログアウト処理部３５から伝達された認証指示中のユーザ名およびパスワードと、内部に登録されているユーザ名およびパスワードとを比較する（Ｓ１６６）。そして、両者が一致した場合（Ｓ１６７でＹＥＳ）、認証成功を利用者認証部３２からログイン・ログアウト処理部３５へ伝達する（Ｓ１６８）。ログイン・ログアウト処理部３５は、遠隔保守コンソール５からの保守対象部３１へのアクセスを許容するためのログイン処理を実行し（Ｓ１６９）、遠隔保守コンソール５へログイン許可を通知する（Ｓ１７０）。これにより、以降、保守作業者は遠隔保守コンソール５からＬＡＮ６経由でクライアント装置３の保守対象部３１へアクセスすることが可能となる。

【００５６】

他方、利用者認証部３２で利用者認証情報が事前に登録されていないと判断されたか（Ｓ１６５でＮＯ）、登録されていたが認証指示中のユーザ名およびパスワードが登録されているユーザ名およびパスワードと一致しないと判断された場合（Ｓ１６７でＮＯ）、認証失敗が利用者認証部３２からログイン・ログアウト処理部３５へ伝達され（Ｓ１７１）、ログイン・ログアウト処理部３５は、遠隔リモート保守コンソール５に対してログイン不許可を通知する（Ｓ１７１）。

【００５７】

図９はログイン中の遠隔保守コンソール５からログアウト要求がＬＡＮ６経由で送信されてきた際のクライアント装置３の処理例を示すフローチャートである。ＬＡＮ６経由でログアウト要求が送信されてきたクライアント装置３は、このログアウト要求をログイン・ログアウト処理部３５で受信し（Ｓ１８１）、遠隔保守コンソール５から保守対象部３１への以後のアクセスを禁止するためのログアウト処理を実行する（Ｓ１８２）。そして、ログイン・ログアウト処理部３５により遠隔保守コンソール５へログアウト完了通知を送信する（Ｓ１８３）。

【００５８】

次に、本実施の形態の動作を説明する。

【００５９】

図１０は本実施の形態の動作例を示すシーケンスチャートであり、以下の４つの場面のシーケンスが示されている。

（１）サーバ側ローカル保守コンソール２からクライアント装置３への利用者認証情報の設定

（２）利用者認証情報登録後の遠隔保守コンソール５によるクライアント装置３へのログイン、ログアウト

（３）サーバ側ローカル保守コンソール２からクライアント装置３への利用者認証情報の無効化

（４）利用者認証情報無効化後の遠隔保守コンソール５によるクライアント装置３へのログイン

【００６０】

以下、上記の４つの場面について本実施の形態の動作を説明する。

【００６１】

（１）先ず、図１、図２、図４および図１０を参照して、サーバ側ローカル保守コンソール２からクライアント装置３へ利用者認証情報を設定する際の動作を説明する。

【００６２】

システム管理者等が、サーバ側ローカル保守コンソール２から、クライアント装置３の保守インタフェース３０のセキュリティを開放するためのユーザ名およびパスワードと対象とするクライアント装置３の指定とを含む利用者認証情報設定要求を入力すると（図１０のＲ１０１）、サーバ装置１でこの要求の受付処理が行われる（Ｒ１０２）。この受付処理では、要求受付部１１が利用者認証情報設定要求を受信する処理とユーザ名およびパスワードの正常性をチェックする処理とが行われる（図２のＳ１０１、Ｓ１０２）。そして問題がなければ、この要求が要求転送部１２に伝達される（図２のＳ１０３）。次に要求転送部１２により、利用者認証情報設定要求中で指定されたクライアント装置３のＩＰアドレスが取得され（図２のＳ１０４）、ＬＡＮ６を経由してクライアント装置３のリモート要求処理部３３へユーザ名およびパスワードを含む利用者認証情報設定指示が送信される（図１０のＲ１０３、図２のＳ１０５）。

【００６３】

クライアント装置３は、サーバ装置１から転送されてきた利用者認証情報設定指示をリモート要求処理部３３で受信し（図４のＳ１２１）、ユーザ名およびパスワードの正常性を確認して（Ｓ１２２）、問題がなければ利用者認証情報設定指示を利用者認証部３２に伝達する（Ｓ１２３）。利用者認証部３２は、利用者認証情報設定指示中のユーザ名およびパスワードを記憶する（図１０のＲ１０４、図２のＳ１２４）。一方、リモート要求処理部３３は、利用者認証情報設定完了通知をＬＡＮ６経由でサーバ装置１の要求転送部１２に送る（図１０のＲ１０５、図２のＳ１２５）。要求転送部１２は、利用者認証情報設定完了通知を受信すると、要求受付部１１を通じてサーバ側ローカル保守コンソール２に出力する（図１０のＲ１０６、図２のＳ１０６～Ｓ１０８）。

【００６４】

（２）次に、図１、図８、図９および図１０を参照して、利用者認証情報登録後の遠隔保守コンソール５によるクライアント装置３へのログイン、ログアウト時の動作を説明する。

【００６５】

クライアント装置３の利用者認証部３２にユーザ名およびパスワードで構成される利用者認証情報が登録された後に、保守作業者が、保守作業の準備の一環として遠隔保守コンソール５からＬＡＮ６経由でクライアント装置３に対して、ユーザ名およびパスワードを指定したログイン要求を入力すると（図１０のＲ１１１）、クライアント装置３で利用者認証にかかる一連の処理が実行される（図１０のＲ１１２、図８のＳ１６１～Ｓ１７２）。具体的には、遠隔保守コンソール５からのログイン要求がログイン・ログアウト処理部３５で受信されて正常性のチェックが行われ（Ｓ１６１、Ｓ１６２）、問題がなければログイン要求中のユーザ名およびパスワードを含む認証指示が利用者認証部３２に出される（Ｓ１６３）。次に利用者認証部３２において、利用者認証情報の登録の有無の判定（Ｓ１６４、Ｓ１６５）、登録がある場合の認証指示中のユーザ名およびパスワードと登録されているユーザ名およびパスワードとの一致の判定（Ｓ１６６、Ｓ１６７）が実施される。図１０の利用者認証Ｒ１１２では、利用者認証情報が事前に登録されており且つログイン要求で指定されたユーザ名およびパスワードが登録されているユーザ名およびパスワードと一致し、認証成功した場面を想定している。このため、利用者認証部３２はログイン・ログアウト処理部３５に認証成功を通知し（Ｓ１６８）、ログイン・ログアウト処理部３５はログイン処理を行い（Ｓ１６９）、遠隔保守コンソール５に対してログイン許可を通知する（Ｓ１７０、図１０のＲ１１３）。これにより、保守作業者は、遠隔保守コンソール５からクライアント装置３の保守対象部３１に対してアクセスし、各種の保守作業を開始することができる。

【００６６】

保守作業者が保守作業を終えたので、遠隔保守コンソール５からログアウト要求を入力すると（図１０のＲ１１４）、クライアント装置３のログイン・ログアウト処理部３５がこれを受信し（図９のＳ１８１）、ログアウト処理を実行する（

Ｓ１８２、図１０のＲ１１５）。そして、ログイン・ログアウト処理部３５は、遠隔保守コンソール５に対してログアウト完了通知を送信する（Ｓ１８３、図１０のＲ１１６）。これにより、遠隔保守コンソール５からのクライアント装置３の保守対象部３１へのアクセスは禁止される。但し、利用者認証部３２にユーザ名およびパスワードが記憶され、ログイン要求待ちとなっているため、クライアント装置３の保守インタフェース３０は開放されている状況である。つまり、クライアント装置３の保守インタフェース３０は閉塞されていない。従って、遠隔保守コンソール５から次のログイン要求が来てユーザ名およびパスワードが一致して認証成功すると、クライアント装置３の保守対象部３１へのアクセスが再び可能となる。

【００６７】

（３）次に、サーバ側ローカル保守コンソール２からクライアント装置３に登録された利用者認証情報を無効化する際の動作を、図１、図３、図５および図１０を参照して説明する。

【００６８】

システム管理者等が、サーバ側ローカル保守コンソール２からクライアント装置３の保守インタフェース３０を閉塞してセキュリティを確保するために、対象となるクライアント装置３を指定した利用者認証情報設定無効要求を入力すると（図１０のＲ１２１）、サーバ装置１で利用者認証情報無効要求受付処理が行われる（Ｒ１２２）。この受付処理では、要求受付部１１が利用者認証情報設定無効要求を受信する処理とこの受信した要求を要求転送部１２に伝達する処理とが行われる（図３のＳ１１１、Ｓ１１２）。次に要求転送部１２により、利用者認証情報設定無効要求中で指定されたクライアント装置３のＩＰアドレスが取得され（図３のＳ１１３）、ＬＡＮ６を経由してクライアント装置３のリモート要求処理部３３へ利用者認証情報設定無効指示が送信される（図１０のＲ１２３、図３のＳ１１４）。

【００６９】

クライアント装置３は、サーバ装置１から転送されてきた利用者認証情報設定無効指示をリモート要求処理部３３で受信し（図５のＳ１３１）、利用者認証情報

設定無効指示を利用者認証部３２に伝達する（Ｓ１３２）。利用者認証部３２は、登録されているユーザ名およびパスワードから構成される利用者認証情報を無効化する（図１０のＲ１２４、図５のＳ１３３）。一方、リモート要求処理部３３は、利用者認証情報設定無効完了通知をＬＡＮ６経由でサーバ装置１の要求転送部１２に送る（図１０のＲ１２５、図５のＳ１３４）。要求転送部１２は、利用者認証情報設定無効完了通知を受信すると、要求受付部１１を通じてサーバ側ローカル保守コンソール２に出力する（図１０のＲ１２６、図３のＳ１１５～Ｓ１１７）。

【００７０】

（４）次に、利用者認証情報無効化後に遠隔保守コンソール５からクライアント装置３へログイン要求があった場合の動作を、図１、図８および図１０を参照して説明する。

【００７１】

遠隔保守コンソール５からＬＡＮ６経由でクライアント装置３に対してログイン要求が入力されると（図１０のＲ１３１）、クライアント装置３で利用者認証にかかる一連の処理が実行される（図１０のＲ１３２、図８のＳ１６１～Ｓ１７２）。しかし、利用者認証部３２には利用者認証情報が登録されていないため、認証失敗となる（図８のＳ１６５でＮＯ）。このため、ログイン・ログアウト処理部３５は、遠隔保守コンソール５に対してログイン不許可を通知する（Ｓ１７２、図１０のＲ１３３）。これにより、遠隔保守コンソール５からのクライアント装置３の保守対象部３１へのアクセスは禁止される。なお、利用者認証部３２にユーザ名およびパスワードが登録されている場合でも、遠隔保守コンソール５からのログイン要求で指定したユーザ名およびパスワードが利用者認証部３２に登録されているユーザ名およびパスワードと一致しないときは同様にログイン・ログアウト処理部３５はログイン許可を与えない動作となる。

【００７２】

図１１は本実施の形態の動作例を示すシーケンスチャートであり、以下の２つの場面のシーケンスが示されている。

（１）クライアント側ローカル保守コンソール４からクライアント装置３への利

用者認証情報の設定

（２）利用者認証登録後の遠隔保守コンソール５によるクライアント装置３へのログイン、ログアウト

（３）クライアント側ローカル保守コンソール４からクライアント装置３への利用者認証情報の無効化

【００７３】

以下、上記の３つの場面について本実施の形態の動作を説明する。

【００７４】

（１）先ず、図１、図６および図１１を参照して、クライアント側ローカル保守コンソール４からクライアント装置３へ利用者認証情報を設定する際の動作を説明する。

【００７５】

システム管理者等が、クライアント側ローカル保守コンソール４から、クライアント装置３の保守インタフェース３０のセキュリティを開放するためのユーザ名およびパスワードの指定を含む利用者認証情報設定要求を入力すると（図１１のＲ１４１）、クライアント装置３は、この利用者認証情報設定要求をローカル要求処理部３４で受信し（図６のＳ１４１）、ユーザ名およびパスワードの正常性を確認して（Ｓ１４２）、問題がなければ利用者認証情報設定指示を利用者認証部３２に伝達する（Ｓ１４３）。利用者認証部３２は、利用者認証情報設定指示中のユーザ名およびパスワードを記憶する（図１１のＲ１４２、図６のＳ１４４）。一方、ローカル要求処理部３４は、利用者認証情報設定完了通知をクライアント側ローカル保守コンソール４に出力する（図１１のＲ１４３、図６のＳ１４５）。

【００７６】

（２）利用者認証登録後の遠隔保守コンソール５によるクライアント装置３へのログイン、ログアウト時の動作は既に説明した図１０のシーケンスＲ１１１～Ｒ１１６と同じであるため、説明は省略する。

【００７７】

（３）次に、クライアント側ローカル保守コンソール４からクライアント装置３

に登録された利用者認証情報を無効化する際の動作を、図１、図７および図１１を参照して説明する。

【００７８】

システム管理者等が、クライアント側ローカル保守コンソール４からクライアント装置３の保守インタフェース３０を閉塞してセキュリティを確保するために、利用者認証情報設定無効要求を入力すると（図１１のＲ１５１）、クライアント装置３は、この利用者認証情報設定無効指示をローカル要求処理部３４で受信し（図７のＳ１５１）、利用者認証情報設定無効指示を利用者認証部３２に伝達する（Ｓ１５２）。利用者認証部３２は、登録されているユーザ名およびパスワードから構成される利用者認証情報を無効化する（図１１のＲ１５２、図７のＳ１５３）。一方、ローカル要求処理部３４は、利用者認証情報設定無効完了通知をクライアント側ローカル保守コンソール４へ出力する（図１１のＲ１５３、図７のＳ１５４）。

【００７９】

以上説明したように、本実施の形態によれば、サーバ側ローカル保守コンソール２から遠隔地にある複数のクライアント装置３の保守インタフェース３０を開放することができ、且つ、サーバ側ローカル保守コンソールから遠隔地にある複数のクライアント装置３の保守インタフェース３０を閉塞することができる。また、クライアント装置３にローカル保守コンソール４が接続されている場合には、各クライアント装置毎に、そのクライアント側ローカル保守コンソール２からクライアント装置３の保守インタフェース３０の開放、閉塞を行うこともできる。

【００８０】

【発明の第２の実施の形態】

図１２を参照すると、本発明の第２の実施の形態にかかるクライアント・サーバ型システムは、図１に示した第１の実施の形態にかかるクライアント・サーバ型システムにおける各クライアント装置３からローカル要求処理部３４を削除し、クライアント側ローカル保守コンソール４からクライアント装置３の利用者認証部３２への利用者認証情報の設定およびその無効化を行えないようにした点で第１の実施の形態と相違し、その他の点は第１の実施の形態と同じである。

【００８１】

本実施の形態においては、サーバ側ローカル保守コンソール２のみからＬＡＮ６を経由してクライアント装置３内に遠隔保守コンソール５からＬＡＮ６を介してクライアント装置３の保守インタフェース３０を開放するための利用者認証情報（ユーザ名およびパスワード）を設定することができ、またサーバ側ローカル保守コンソール２からクライアント装置３に設定した利用者認証情報を削除し、クライアント装置３の保守インタフェース３０を利用禁止にすることができる。

【００８２】

このようにサーバ側ローカル保守コンソール２のみに限定して複数のクライアント装置３の保守インタフェース３０を開放、閉塞できるようにしたことで、保守インタフェース３０のセキュリティの管理をサーバ装置１のシステム管理者が容易に管理することが可能となる。

【００８３】

【発明の第３の実施の形態】

図１３を参照すると、本発明の第３の実施の形態にかかるクライアント・サーバ型システムは、図１２に示した第２の実施の形態にかかるクライアント・サーバ型システムにおけるサーバ装置１３に、ユーザ名およびパスワードを暗号化する暗号化部１３を備え、各クライアント装置３に、暗号化されたユーザ名およびパスワードを復号化する復号化部３６を備えている点で第２の実施の形態と相違し、その他の点は第２の実施の形態と同じである。

【００８４】

図１４はサーバ側ローカル保守コンソール２から利用者認証情報設定要求が入力された際のサーバ装置１の処理例を示すフローチャートであり、ステップＳ３０１～Ｓ３０３が追加されている点が図３のフローチャートと相違する。システム管理者等が、利用者認証情報の設定対象となるクライアント装置３の指定情報と、設定したい利用者認証情報としてのユーザ名およびパスワードとを含む利用者認証情報設定要求をサーバ側ローカル保守コンソール２から入力すると、要求受付部１１がこの要求を受信し（Ｓ１０１）、ユーザ名およびパスワードの桁数などの正常性をチェックし（Ｓ１０２）、問題がなければ受け付けた利用者認証情

報設定要求中のユーザ名およびパスワードを要求受付部１１から暗号化部１３へ伝達する（Ｓ３０１）。暗号化部１３は、共通鍵暗号方法や秘密鍵暗号方法などシステムで予め定められた任意の暗号方法により、ユーザ名およびパスワードを暗号化し（Ｓ３０２）、暗号化されたユーザ名およびパスワードを要求受付部１１に伝達する（Ｓ３０３）。要求受付部１１は、暗号化されたユーザ名およびパスワードを含む利用者認証情報設定要求を要求転送部１２へ伝達する（Ｓ１０３）。以下、図３を参照して説明した処理と同様の処理が実行される（Ｓ１０４～Ｓ１０８）。

【００８５】

図１５はサーバ装置１から利用者認証情報設定指示がＬＡＮ６経由で送信されてきた際のクライアント装置３の処理例を示すフローチャートであり、ステップＳ３１１～Ｓ３１３が追加されている点が図４のフローチャートと相違する。ＬＡＮ経由で利用者認証情報設定指示が送信されてきたクライアント装置３は、この指示をリモート要求処理部３３で受信し（Ｓ１２１）、指示中の暗号化されたユーザ名およびパスワードを復号化部３６へ伝達する（Ｓ３１１）。復号化部３６は、暗号化されたユーザ名およびパスワードを復号化し（Ｓ３１２）、リモート要求処理部３３へ伝達する（Ｓ３１３）。リモート要求処理部３３は、ユーザ名およびパスワードが所定の桁数を満たすかどうかのチェックを行い（Ｓ１２２）、問題がなければ、この指示を利用者認証部３２に伝達する（Ｓ１２３）。以下、図４を参照して説明した処理と同様の処理が実行される（Ｓ１２４、Ｓ１２５）。

【００８６】

次に、本実施の形態の動作を説明する。

【００８７】

図１６は本実施の形態の動作例を示すシーケンスチャートであり、サーバ側ローカル保守コンソール２からクライアント装置３への利用者認証情報の設定場面のシーケンスを示す。以下、図１３～図１６を参照して、サーバ側ローカル保守コンソール２からクライアント装置３へ利用者認証情報を設定する際の動作を説明する。

【００８８】

システム管理者等が、サーバ側ローカル保守コンソール２から、クライアント装置３の保守インタフェース３０のセキュリティを開放するためのユーザ名およびパスワードと対象とするクライアント装置３の指定とを含む利用者認証情報設定要求を入力すると（図１６のＲ３０１）、サーバ装置１でこの要求の受付処理が行われる（Ｒ３０２）。この受付処理では、要求受付部１１が利用者認証情報設定要求を受信する処理とユーザ名およびパスワードの正常性をチェックする処理とが行われる（図１４のＳ１０１、Ｓ１０２）。そして問題がなければ、暗号化部１３でユーザ名およびパスワードを暗号化する処理が実施される（図１４のＲ３０３、図１４のＳ３０１～Ｓ３０３）。そして、暗号化されたユーザ名およびパスワードを含む利用者認証情報設定要求が要求受付部１１から要求転送部１１へ伝達される（Ｓ１０３）。その後、要求転送部１２は、利用者認証情報設定要求中で指定されたクライアント装置３のＩＰアドレスを取得し（Ｓ１０４）、ＬＡＮ６を経由してクライアント装置３のリモート要求処理部３３へユーザ名およびパスワードを含む利用者認証情報設定指示を送信する（図１６のＲ３０４、図１４のＳ１０５）。

【００８９】

クライアント装置３は、サーバ装置１から転送されてきた利用者認証情報設定指示をリモート要求処理部３３で受信し（図１５のＳ１２１）、指示中に含まれる暗号化されたユーザ名およびパスワードを復号化部３６を用いて復号化する（図１６のＲ３０５、図１５のＳ３１１～Ｓ３１３）。続いて、復号化されたユーザ名およびパスワードの正常性を確認し（Ｓ１２２）、問題がなければ利用者認証情報設定指示を利用者認証部３２に伝達する（Ｓ１２３）。利用者認証部３２は、利用者認証情報設定指示中のユーザ名およびパスワードを記憶する（図１６のＲ３０６、図１５のＳ１２４）。一方、リモート要求処理部３３は、利用者認証情報設定完了通知をＬＡＮ６経由でサーバ装置１の要求転送部１２に送る（図１６のＲ３０７、図１５のＳ１２５）。要求転送部１２は、利用者認証情報設定完了通知を受信すると、要求受付部１１を通じてサーバ側ローカル保守コンソール２に出力する（図１６のＲ３０８、図１４のＳ１０６～Ｓ１０８）。

【００９０】

保守者が保守コンソール５を使用してログイン・ログアウトする手順及びサーバ側ローカル保守コンソール２から設定済みのユーザ名・パスワードを無効にする手順など、その他の動作は第２の実施の形態と同様である。

【００９１】

以上説明したように本実施の形態によれば、サーバ側ローカル保守コンソール２から複数のクライアント装置３の保守インタフェース３０を開放する際に、サーバ装置１とクライアント装置３間で転送するユーザ名およびパスワードから構成される利用者認証情報を暗号化することにより、利用者認証情報の漏洩が防止でき、セキュリティを確保することができる。

【００９２】

なお、本実施の形態において、第１の実施の形態と同様にそれぞれのクライアント装置３に図１のクライアント側ローカル保守コンソール４を接続し、クライアント装置３内にローカル要求処理部３４を設けるようにしても良い。

【００９３】

【発明の第４の実施の形態】

図１７を参照すると、本発明の第４の実施の形態にかかるクライアント・サーバ型システムは、図１３に示した第３の実施の形態にかかるクライアント・サーバ型システムにおける各クライアント装置３に、利用者認証部３２の利用者認証情報が再設定される際にクライアント装置３の保守インタフェース３０を利用するログイン中の装置があれば該装置に対して強制切断通知を送出して強制切断を実施する強制切断部３７を備えている点で第３の実施の形態と相違し、その他の点は第３の実施の形態と同じである。

【００９４】

図１８はサーバ装置１から利用者認証情報設定指示がＬＡＮ６経由で送信されてきた際のクライアント装置３の処理例を示すフローチャートであり、ステップＳ４０１～Ｓ４０５が追加されている点が図１５のフローチャートと相違する。ＬＡＮ経由で利用者認証情報設定指示が送信されてきたクライアント装置３は、この指示をリモート要求処理部３３で受信し（Ｓ１２１）、この指示中の暗号化さ

れたユーザ名およびパスワードを復号化部３６で復号化し（Ｓ３１１～Ｓ３１３）、ユーザ名およびパスワードが所定の桁数を満たすかどうかのチェックを行い（Ｓ１２２）、問題がなければ、ユーザ名およびパスワードを含む利用者認証情報設定指示をリモート要求処理部３３から利用者認証部３２に伝達する（Ｓ１２３）。ここまでは第３の実施の形態と同じ動作である。続いて、利用者認証部３２により利用者認証情報が既に登録されているかどうかを判定し（Ｓ４０１）、未登録の場合と既登録の場合とで処理を切り分ける。

【００９５】

利用者認証情報が利用者認証部３２に未だ登録されていないときは、速やかに、利用者認証情報設定指示中のユーザ名およびパスワードを利用者認証部３２に登録し（Ｓ１２４）、リモート要求処理部３３から利用者認証情報設定完了通知をサーバ装置１に送信する（Ｓ１２５）。

【００９６】

他方、利用者認証情報が利用者認証部３２に既に登録されていた場合、利用者認証部３２から強制切断部３７に対し強制切断処理を依頼する（Ｓ４０２）。強制切断部３７は、ログイン・ログアウト処理部３５に対してクライアント装置３の保守インタフェース３０を利用するためにログインしている遠隔保守コンソール５が存在するかどうかを問い合わせ（Ｓ４０３）、存在しない場合には処理完了を利用者認証部３２に通知する（Ｓ４０５）。しかし、ログイン中の遠隔保守コンソール５が存在する場合は、その遠隔保守コンソール５に対して強制切断通知を送出し、強制切断を行う（Ｓ４０４）、そして、処理完了を利用者認証部３２に通知する（Ｓ４０５）。その後、利用者認証部３２は、利用者認証情報設定指示中のユーザ名およびパスワードを利用者認証部３２に登録し（Ｓ１２４）、リモート要求処理部３３から利用者認証情報設定完了通知をサーバ装置１に送信する（Ｓ１２５）。

【００９７】

次に本実施の形態の動作を説明する。

【００９８】

図１９は本実施の形態の動作例を示すシーケンスチャートであり、サーバ側ロー

カル保守コンソール２からＬＡＮ６を経由してクライアント装置３内にクライアント装置３の保守インタフェース３０を開放するためのユーザ名およびパスワードの初期設定を行った後、何者かが遠隔保守コンソール５からクライアント装置３にログインして保守対象部３４にアクセスしている状態で、サーバ側ローカル保守コンソール２からクライアント装置３の保守インタフェース３０のユーザ名およびパスワードを再設定し、正規の遠隔保守を行う場面のシーケンスを示す。

【００９９】

図１９のシーケンスのうち、サーバ側ローカル保守コンソール２からクライアント装置３にユーザ名およびパスワードを初期設定するシーケンスＲ３０１～Ｒ３０８は、図１６を参照して説明した処理と同じである。この場合、設定前の利用者認証部３２にはユーザ名およびパスワードが存在しないので、図１８の処理Ｓ４０２～Ｓ４０５はスキップされる。

【０１００】

クライアント装置３の利用者認証部３２にユーザ名およびパスワードが設定された後、何者かが遠隔保守コンソール５からＬＡＮ６経由でクライアント装置３に対してユーザ名およびパスワードを指定したログイン要求を入力すると（図１９のＲ４０１）、図８および図１０を参照して説明した処理と同様の処理がクライアント装置３で実施され、ログイン要求中のユーザ名およびパスワードが利用者認証部３２に登録されているユーザ名およびパスワードと一致すると、ログインが許可され（図１９のＲ４０２、Ｒ４０３）、遠隔保守コンソール５からクライアント装置３の保守対象部３１に対するアクセスが可能となる。

【０１０１】

このように遠隔保守コンソール５がログインしている最中に、サーバ側ローカル保守コンソール２から利用者認証情報設定要求が入力さたた場合（図１９のＲ４１１）、以下のような動作が行われる。

【０１０２】

先ず、サーバ装置１の要求受付部１１が利用者認証情報設定要求をサーバ側ローカル保守コンソール２から受信し、その正常性をチェックする受付処理を行う（図１９のＲ４１２）。続いて、暗号化部１３でユーザ名およびパスワードが暗号

化され（図１９のＲ４１３）、暗号化されたユーザ名およびパスワードを含む利用者認証情報設定指示が、要求転送部１２からＬＡＮ６を経由してクライアント装置３のリモート要求処理部３３へ送信される（図１９のＲ４１４）。

【０１０３】

クライアント装置３は、サーバ装置１から転送されてきた利用者認証情報設定指示をリモート要求処理部３３で受信し（図１８のＳ１２１）、指示中に含まれる暗号化されたユーザ名およびパスワードを復号化部３６を用いて復号化する（図１９のＲ４１５、図１８のＳ３１１～Ｓ３１３）。続いて、復号されたユーザ名およびパスワードの正常性を確認し（Ｓ１２２）、問題がなければ利用者認証情報設定指示を利用者認証部３２に伝達する（Ｓ１２３）。

【０１０４】

利用者認証部３２は、利用者認証情報が既に登録されているため（Ｓ４０１でＹＥＳ）、強制切断部３７に対し強制切断処理を依頼する（Ｓ４０２）。強制切断部３７は、ログイン・ログアウト処理部３５において遠隔保守コンソール５がログイン中であることを確認し（Ｓ４０３でＹＥＳ）、遠隔保守コンソール５に対して強制切断通知を送出し、強制切断を行う（図１９のＲ４１６、図１８のＳ４０４）、これにより、遠隔保守コンソール５からの保守対象部３１へのアクセスは不可能になる。その後、強制切断部３７は、処理完了を利用者認証部３２に通知し（Ｓ４０５）、利用者認証部３２は、既に登録されている利用者認証情報を消去する等して無効化した後、利用者認証情報設定指示中のユーザ名およびパスワードを登録する（図１９のＲ４１７、図１８のＳ１２４）。そして、リモート要求処理部３３から利用者認証情報設定完了通知がサーバ装置１に送信され（図１９のＲ４１８、図１８のＳ１２５）、最終的にサーバ側ローカル保守コンソール２へ通知される（図１９のＲ４１９）。

【０１０５】

ユーザ名およびパスワードが再設定された後、保守者が再設定された新たなユーザ名およびパスワードを使って遠隔保守コンソール５からクライアント装置３にログインして保守作業を行い、作業終了時点でログアウトを行う場面のシーケンスＲ１１１～Ｒ１１６は、図１０を参照して説明したシーケンスと同じである。

【０１０６】

このように本実施の形態によれば、サーバ側ローカル保守コンソール２からクライアント装置３の保守インタフェース３０のユーザ名およびパスワードを設定する指示があった場合、クライアント装置３は、利用者認証部３２に既に利用者認証情報が設定されているときは、遠隔保守コンソール５がログイン中であれば強制切断通知を送出して強制切断を行うと共に、利用者認証部３２にユーザ名およびパスワードを再設定する。従って、クライアント装置３の保守インタフェース３０に対して悪意のアクセスが行われているなどの場合に、サーバ側ローカル保守コンソール２からクライアント装置１の保守インタフェース３０のユーザ名およびパスワードを再度設定し直すことで、悪意のアクセスを阻止することができ、同時にユーザ名およびパスワードを再設定することができ、充分なセキュリティを確保することができる。

【０１０７】

なお、本実施の形態において、第１の実施の形態と同様にそれぞれのクライアント装置３に図１のクライアント側ローカル保守コンソール４を接続し、クライアント装置３内にローカル要求処理部３４を設けるようにしても良い。また、利用者認証情報を暗号化せずにサーバ装置１からクライアント装置３へ転送するようにしても良く、その場合には暗号化部１３および復号化部３６は省略される。

【０１０８】

【発明の第５の実施の形態】

図２０を参照すると、本発明の第５の実施の形態にかかるクライアント・サーバ型システムは、図１７に示した第４の実施の形態にかかるクライアント・サーバ型システムにおけるサーバ装置１に、サーバ側ローカル保守コンソール２からの利用可能時間の設定要求の受付けとクライアント装置３への転送の機能を持たせた点と、各クライアント装置３に、遠隔保守コンソール５からの保守インタフェース３０の利用時間を管理し、サーバ装置１から事前に設定された利用可能時間を超える場合には遠隔保守コンソール５に対して利用時間終了通知を送出して強制切断すると共に、利用者認識部３２に登録されている利用者認証情報を無効化する利用時間管理部３８を備えている点で、第４の実施の形態と相違し、その他

は第４の実施の形態と同じである。

【０１０９】

図２１はサーバ側ローカル保守コンソール２から利用者認証情報設定要求が入力された際のサーバ装置１の処理例を示すフローチャートである。システム管理者等が、利用者認証情報の設定対象となるクライアント装置３の指定情報と、設定したい利用者認証情報としてのユーザ名およびパスワードと、設定したい利用可能時間とを指定した利用者認証情報設定要求をサーバ側ローカル保守コンソール２から入力すると、要求受付部１１がこの要求を受信し（Ｓ５０１）、ユーザ名、パスワードおよび利用可能時間の桁数などの正常性をチェックする（Ｓ５０２）。桁数などが所定の条件を満足しない場合、要求は拒否される。問題がなければ、受け付けた利用者認証情報設定要求中のユーザ名およびパスワードを暗号化部１３において暗号化し（Ｓ５０３～Ｓ５０５）、暗号化されたユーザ名およびパスワードと利用可能時間を含む利用者認証情報設定要求を要求転送部１２へ伝達する（Ｓ５０６）。次に、要求転送部１２により、利用者認証情報設定要求中で指定されているクライアント装置３のＩＰアドレスを取得し（Ｓ５０７）、このＩＰアドレスを用いて利用者認証情報設定要求中の暗号化されたユーザ名およびパスワードと利用可能時間を含む利用者認証情報設定指示をＬＡＮ６経由で対象クライアント装置３へ送信する（Ｓ５０８）。そして、対象クライアント装置３から利用者認証情報設定完了通知が返されてくると、この通知を要求転送部１２で受信し、要求受付部１１経由でサーバ側ローカル保守コンソール２に利用者認証情報設定完了通知を出力する（Ｓ５０９～Ｓ５１１）。

【０１１０】

図２２はサーバ装置１から利用者認証情報設定指示がＬＡＮ６経由で送信されてきた際のクライアント装置３の処理例を示すフローチャートであり、ステップＳ５２１、Ｓ５２２、Ｓ５２３が追加されている点が図１８のフローチャートと相違する。ＬＡＮ経由で利用者認証情報設定指示が送信されてきたクライアント装置３は、この指示をリモート要求処理部３３で受信し（Ｓ１２１）、この指示中の暗号化されたユーザ名およびパスワードを復号化部３６で復号化し（Ｓ３１１～Ｓ３１３）、ユーザ名、パスワードおよび利用可能時間が所定の桁数を満たす

かどうかのチェックを行い（Ｓ１２２）、問題がなければ、利用可能時間を利用時間管理部３８に伝達する（Ｓ５２１）。利用時間管理部３８は、この利用可能時間を記憶する（Ｓ５２２）。他方、リモート要求処理部３３は、ユーザ名およびパスワードを含む利用者認証情報設定指示を利用者認証部３２に伝達する（Ｓ１２３）。以降、図１８と同様の処理が行われ（Ｓ４０１～Ｓ４０５、Ｓ１２４、Ｓ１２５）、利用者認証情報が利用者認証部３２に記憶されて保守インタフェース３０が開放された時点で、利用時間管理部３８は記憶した利用可能時間に従って、利用時間の管理を開始する（Ｓ５２３）。

【０１１１】

図２３は利用時間管理部３８が利用時間の管理を開始した後の処理例を示すフローチャートである。利用時間管理部３８は利用時間の管理を開始すると、内部に記録されている利用可能時間を時間の経過に応じて減算していき、残り利用時間が０になったかどうか、つまり事前に設定された利用可能時間が経過したかどうかを判定する（Ｓ５４１）。そして、残り利用時間が０になると、ログイン中の遠隔保守コンソール５が存在する場合（Ｓ５４２でＹＥＳ）、ログイン中の遠隔保守コンソール５に対して利用時間終了通知を送信し、強制切断を行う（Ｓ５４３）。ログイン中の遠隔保守コンソール５が存在しない場合には、このステップＳ５４３はスキップされる。次に利用時間管理部３８は、利用者認証部３２に対して利用者認証情報の無効化を指示し、それに応じて利用者認証部３２が登録されている利用者認証情報を無効化する（Ｓ５４４）。その後、利用時間管理部３８が初期化される（Ｓ５４５）。

【０１１２】

図２４は本実施の形態の動作例を示すシーケンスチャートであり、以下の２つの場面のシーケンスが示されている。

（１）サーバ側ローカル保守コンソール２からクライアント装置３への利用者認証情報および利用可能時間の設定

（２）遠隔保守コンソール５によるクライアント装置３へのログイン

【０１１３】

以下、上記の２つの場面について本実施の形態の動作を説明する。

【０１１４】

（１）先ず、図２０～図２４を参照して、サーバ側ローカル保守コンソール２からクライアント装置３へ利用者認証情報および利用可能時間を設定する際の動作を説明する。

【０１１５】

システム管理者等が、サーバ側ローカル保守コンソール２から、クライアント装置３の保守インタフェース３０のセキュリティを開放するためのユーザ名およびパスワードと、対象とするクライアント装置３の指定と、利用可能時間とを含む利用者認証情報設定要求を入力すると（図２４のＲ５０１）、サーバ装置１でこの要求の受付処理が行われる（Ｒ５０２）。この受付処理では、要求受付部１１が利用者認証情報設定要求を受信する処理とユーザ名、パスワードおよび利用可能時間の正常性をチェックする処理とが行われる（図２１のＳ５０１、Ｓ５０２）。そして問題がなければ、暗号化部１３でユーザ名およびパスワードを暗号化する処理が実施される（図２４のＲ５０３、図２１のＳ５０３～Ｓ５０５）。そして、暗号化されたユーザ名およびパスワードならびに利用可能時間を含む利用者認証情報設定要求が要求受付部１１から要求転送部１１へ伝達される（Ｓ５０６）。その後、要求転送部１２は、利用者認証情報設定要求中で指定されたクライアント装置３のＩＰアドレスを取得し（Ｓ５０７）、ＬＡＮ６を経由してクライアント装置３のリモート要求処理部３３へ暗号化されたユーザ名およびパスワードならびに利用可能時間を含む利用者認証情報設定指示を送信する（図２４のＲ５０４、図２１のＳ５０８）。

【０１１６】

クライアント装置３は、サーバ装置１から転送されてきた利用者認証情報設定指示をリモート要求処理部３３で受信し（図２２のＳ１２１）、指示中に含まれる暗号化されたユーザ名およびパスワードを復号化部３６を用いて復号化する（図２４のＲ５０５、図２２のＳ３１１～Ｓ３１３）。続いて、復号化されたユーザ名およびパスワードならびに利用可能時間の正常性を確認し（Ｓ１２２）、問題がなければ、先ず利用可能時間を利用時間管理部３８に伝達する（Ｓ５２１）。利用時間管理部３８はこの利用可能時間を記憶する（図２４のＲ５０６、図２２

のＳ５２２）。次にリモート要求処理部３３は、ユーザ名およびパスワードを含む利用者認証情報設定指示を利用者認証部３２に伝達する（Ｓ１２３）。以降、図１８を参照して説明した処理と同様の処理が行われ（Ｓ４０１～Ｓ４０５、Ｓ１２４、Ｓ１２５）、利用者認証部３２にユーザ名とパスワードが設定され（図２４のＲ５０７）、また利用者認証情報設定完了通知がクライアント装置３からサーバ側リモート保守コンソール２へ通知される（Ｒ５０８、Ｒ５０９）。そして、利用時間管理部３８が利用時間の管理を開始する（Ｒ５１０、図２２のＳ５２３）。

【０１１７】

（２）次に、遠隔保守コンソール５から何者かがクライアント装置３へログインしたときの動作を、図２３および図２４を参照して説明する。

【０１１８】

クライアント装置３の利用者認証部３２にユーザ名およびパスワードが設定され、また利用時間管理部３８で利用時間の管理が開始された後、何者かが遠隔保守コンソール５からＬＡＮ６経由でクライアント装置３に対してユーザ名およびパスワードを指定したログイン要求を入力すると（図２４のＲ５１１）、図８および図１０を参照して説明した処理と同様の処理がクライアント装置３で実施され、ログイン要求中のユーザ名およびパスワードが利用者認証部３２に登録されているユーザ名およびパスワードと一致すると、ログインが許可され（図２４のＲ５１２、Ｒ５１３）、遠隔保守コンソール５からクライアント装置３の保守対象部３１に対するアクセスが可能となる。

【０１１９】

しかし、遠隔保守コンソール５からログイン・ログアウト処理部３５に対してログアウト要求が入力される前に利用可能時間が経過した場合（図２４のＲ５１５、図２３のＳ５４１およびＳ５４２でＹＥＳ）、利用時間管理部３５は、遠隔保守コンソール５に対して利用時間終了通知を送信し、強制切断を行う（図２４のＲ５１６、図２３のＳ５４３）。また利用時間管理部３８は、利用者認証部３２に対して利用者認証情報の無効化を指示し、利用者認証部３２は登録されている利用者認証情報を無効化する（図２４のＲ５１７、図２３のＳ５４４）。

【０１２０】

以上説明したように本実施の形態によれば、サーバ側ローカル保守コンソール２から利用可能時間を指定して、クライアント装置３の保守インタフェース３０の利用時間を管理することができる。従って、クライアント装置３の保守インタフェース３０が一度開放された後、保守インタフェース３０が長時間開放し続け、悪意のアクセスの危険性が高くなることを防ぐことができる。

【０１２１】

なお、本実施の形態では、サーバ側ローカル保守コンソール２からクライアント装置３に利用者認証情報を設定する指示で利用可能時間を併せて設定するように指示したが、サーバ側ローカル保守コンソール２からクライアント装置３への利用者認証情報の設定指示と、サーバ側ローカル保守コンソール２からクライアント装置３への利用可能時間の設定指示とを独立させるようにしても良い。また、サーバ側ローカル保守コンソール２からクライアント装置３への利用可能時間の設定機能を無くし、利用時間管理部３８に予め記憶された固定の利用可能時間を使用するようにしても良い。

【０１２２】

また、本実施の形態において、第１の実施の形態と同様にそれぞれのクライアント装置３に図１のクライアント側ローカル保守コンソール４を接続し、クライアント装置３内にローカル要求処理部３４を設けるようにしても良い。さらに、利用者認証情報を暗号化せずにサーバ装置１からクライアント装置３へ転送するようにしても良く、その場合には暗号化部１３および復号化部３６は省略される。また、利用者認証情報の再設定時にログイン中の遠隔保守コンソール５を強制切断しないようにしても良く、その場合には強制切断部３７は省略される。

【０１２３】

【発明の第６の実施の形態】

図２５を参照すると、本発明の第６の実施の形態にかかるクライアント・サーバ型システムは、図２０に示した第５の実施の形態にかかるクライアント・サーバ型システムにおけるサーバ装置１に、サーバ側ローカル保守コンソール２からのログイン可能回数の要求の受け付けとクライアント装置３への転送の機能を持た

せた点と、各クライアント装置３に、遠隔保守コンソール５からのログイン回数を管理し、サーバ装置１から設定されたログイン可能回数を超過した場合にはログインを許可せず遠隔保守コンソール５に対して利用回数終了通知を送出すると共に、利用者認識部３２に登録されている利用者認証情報を無効化するログイン回数管理部３９を備えている点で、第５の実施の形態と相違し、その他は第５の実施の形態と同じである。

【０１２４】

図２６はサーバ側ローカル保守コンソール２から利用者認証情報設定要求が入力された際のサーバ装置１の処理例を示すフローチャートである。システム管理者等が、利用者認証情報の設定対象となるクライアント装置３の指定情報と、設定したい利用者認証情報としてのユーザ名およびパスワードと、設定したい利用可能時間と、設定したいログイン可能回数とを指定した利用者認証情報設定要求をサーバ側ローカル保守コンソール２から入力すると、要求受付部１１がこの要求を受信し（Ｓ６０１）、ユーザ名、パスワード、利用可能時間およびログイン可能回数の桁数などの正常性をチェックする（Ｓ６０２）。桁数などが所定の条件を満足しない場合、要求は拒否される。問題がなければ、受け付けた利用者認証情報設定要求中のユーザ名およびパスワードを暗号化部１３において暗号化し（Ｓ６０３～Ｓ６０５）、暗号化されたユーザ名およびパスワードと利用可能時間ならびにログイン可能回数を含む利用者認証情報設定要求を要求転送部１２へ伝達する（Ｓ６０６）。次に、要求転送部１２により、利用者認証情報設定要求中で指定されているクライアント装置３のＩＰアドレスを取得し（Ｓ６０７）、このＩＰアドレスを用いて利用者認証情報設定要求中の暗号化されたユーザ名およびパスワードと利用可能時間ならびにログイン可能回数を含む利用者認証情報設定指示をＬＡＮ６経由で対象クライアント装置３へ送信する（Ｓ６０８）。そして、対象クライアント装置３から利用者認証情報設定完了通知が返されてくると、この通知を要求転送部１２で受信し、要求受付部１１経由でサーバ側ローカル保守コンソール２に利用者認証情報設定完了通知を出力する（Ｓ６０９～Ｓ６１１）。

【０１２５】

図２７はサーバ側ローカル保守コンソール２から利用者認証情報設定要求が入力された際のサーバ装置１の処理例を示すフローチャートであり、ステップＳ６２１、Ｓ６２２が追加されている点が図２２のフローチャートと相違する。ＬＡＮ経由で利用者認証情報設定指示が送信されてきたクライアント装置３は、この指示をリモート要求処理部３３で受信すると（Ｓ１２１）、この指示中の暗号化されたユーザ名およびパスワードを復号化部３６で復号化し（Ｓ３１１～Ｓ３１３）、ユーザ名、パスワード、利用可能時間およびログイン可能回数が所定の桁数を満たすかどうかのチェックを行う（Ｓ１２２）。問題がなければ、利用可能時間を利用時間管理部３８に伝達し（Ｓ５２１）、利用時間管理部３８はこの利用可能時間を記憶する（Ｓ５２２）。さらに、ログイン可能回数をログイン回数管理部３９に伝達し（Ｓ６２１）、ログイン回数管理部３９はこのログイン可能回数を記憶する（Ｓ６２２）。以降、図２２と同様の処理が行われる（Ｓ１２３、Ｓ４０１～Ｓ４０５、Ｓ１２４、Ｓ１２５、Ｓ５２３）。

【０１２６】

図２８は遠隔保守コンソール５からユーザ名およびパスワードの指定を含むログイン要求がＬＡＮ６経由で送信されてきた際のクライアント装置３の処理例を示すフローチャートであり、ステップＳ６３１～Ｓ６３５が追加されている点が図８のフローチャートと相違する。本実施の形態においては、ログイン・ログアウト処理部３５で遠隔保守コンソール５からのログイン要求を受信すると（Ｓ１６１）、ログイン回数管理部３９でログイン回数を＋１し（Ｓ６３１）、事前に設定されたログイン可能回数を超えたかどうかを判定する（Ｓ６３２）。ログイン可能回数を超えていない場合は図８と同様の処理が行われる（Ｓ１６２～Ｓ１７２）。

【０１２７】

他方、ログイン回数がログイン可能回数を超えていた場合は、ログイン回数管理部３９からログイン要求を出した遠隔保守コンソール５に対して利用回数終了通知を送出する（Ｓ６３３）。このときログイン・ログアウト処理部３５はログイン許可を与えない。さらに利用者認証部３２は、登録されている利用者認証情報を無効化する（Ｓ６３４）。そして、ログイン回数管理部３８が初期化される（

Ｓ６３５）。

【０１２８】

図２９は本実施の形態の動作例を示すシーケンスチャートであり、以下の２つの場面のシーケンスが示されている。

（１）サーバ側ローカル保守コンソール２からクライアント装置３への利用者認証情報および利用可能時間ならびにログイン可能回数の設定

（２）遠隔保守コンソール５からのクライアント装置３への頻繁なログイン

【０１２９】

以下、上記の２つの場面について本実施の形態の動作を説明する。

【０１３０】

（１）先ず、図２５～図２７および図２９を参照して、サーバ側ローカル保守コンソール２からクライアント装置３へ利用者認証情報、利用可能時間およびログイン可能回数を設定する際の動作を説明する。

【０１３１】

システム管理者等が、サーバ側ローカル保守コンソール２から、クライアント装置３の保守インタフェース３０のセキュリティを開放するためのユーザ名およびパスワードと、対象とするクライアント装置３の指定と、許容するログイン最大時間である利用可能時間と、この利用可能時間内における最大ログイン可能回数であるログイン可能回数とを含む利用者認証情報設定要求を入力すると（図２９のＲ６０１）、サーバ装置１でこの要求の受付処理が行われる（Ｒ６０２）。この受付処理では、要求受付部１１が利用者認証情報設定要求を受信する処理とユーザ名、パスワード、利用可能時間およびログイン可能回数の正常性をチェックする処理とが行われる（図２６のＳ６０１、Ｓ６０２）。そして問題がなければ、暗号化部１３でユーザ名およびパスワードを暗号化する処理が実施される（図２９のＲ６０３、図２６のＳ６０３～Ｓ６０５）。そして、暗号化されたユーザ名およびパスワードと利用可能時間およびログイン可能回数を含む利用者認証情報設定要求が要求受付部１１から要求転送部１１へ伝達される（Ｓ６０６）。その後、要求転送部１２は、利用者認証情報設定要求中で指定されたクライアント装置３のＩＰアドレスを取得し（Ｓ６０７）、ＬＡＮ６を経由してクライアント

装置３のリモート要求処理部３３へ暗号化されたユーザ名およびパスワードならびに利用可能時間を含む利用者認証情報設定指示を送信する（図２９のＲ６０４、図２６のＳ６０８）。

【０１３２】

クライアント装置３は、サーバ装置１から転送されてきた利用者認証情報設定指示をリモート要求処理部３３で受信し（図２７のＳ１２１）、指示中に含まれる暗号化されたユーザ名およびパスワードを復号化部３６を用いて復号化する（図２９のＲ６０５、図２７のＳ３１１～Ｓ３１３）。続いて、復号されたユーザ名およびパスワードと利用可能時間およびログイン可能回数の正常性を確認し（Ｓ１２２）、問題がなければ、利用可能時間を利用時間管理部３８に、ログイン可能回数をログイン回数管理部３９にそれぞれ伝達し、利用時間管理部３８が利用可能時間を、ログイン回数管理部３９がログイン可能回数をそれぞれ記憶する（図２９のＲ６０６、図２７のＳ５２１、Ｓ５２２、Ｓ６２１、Ｓ６２２）。次にリモート要求処理部３３は、ユーザ名およびパスワードを含む利用者認証情報設定指示を利用者認証部３２に伝達する（Ｓ１２３）。以降、図２２と同様の処理が行われ（Ｓ４０１～Ｓ４０５、Ｓ１２４、Ｓ１２５、Ｓ５２３）、利用者認証部３２にユーザ名とパスワードが設定され（図２９のＲ６０７）、また利用者認証情報設定完了通知がクライアント装置３からサーバ側リモート保守コンソール２へ通知される（Ｒ６０８、Ｒ６０９）。さらに、利用時間管理部３８が利用時間の管理を開始する（Ｒ６１０）。

【０１３３】

（２）次に、遠隔保守コンソール５から保守作業者がクライアント装置３へ頻繁にログインしたときの動作を、図２５、図２８および図２９を参照して説明する。

【０１３４】

クライアント装置３の利用者認証部３２にユーザ名およびパスワードが設定され、利用時間管理部３８に利用可能時間が設定され、さらにログイン回数管理部３９にログイン可能回数が設定された後、何者かが遠隔保守コンソール５からＬＡＮ６経由でクライアント装置３に対してユーザ名およびパスワードを指定したロ

グイン要求を入力すると（図２９のＲ６１１）、ログイン回数管理部３９でログイン回数が更新され（図２９のＲ６１２、図２８のＳ６３１）、また利用者認証処理Ｒ６１３が実施され、ログイン要求中のユーザ名およびパスワードが利用者認証部３２に登録されているユーザ名およびパスワードと一致すると、ログインが許可される（図２９のＲ６１４）。これにより、遠隔保守コンソール５からクライアント装置３の保守対象部３１に対するアクセスが可能となる。その後、図３０のシーケンスでは、遠隔保守コンソールがログアウトし、再びログインしている。

【０１３５】

第５の実施の形態では利用可能時間以内であれば遠隔保守コンソール５からユーザ名およびパスワードを使ってログイン、ログアウトを何度も繰り返すことができた。しかし、本実施の形態の場合、ログイン要求がある毎にログイン回数管理部３９がログイン回数を更新し、ログイン回数が事前に設定されたログイン可能回数を超えると（図２９のＲ６２１、図２８のＳ６３２でＹＥＳ）、利用可能時間が終了する前であっても、利用回数終了通知を遠隔保守コンソール５へ通知し（図２９のＲ６２２、図２８のＳ６３３）、ログインを許可しない。また、利用者認証部３２は登録されているユーザ名およびパスワードを無効とする（図２９のＲ６２３、図２８のＳ６３４）。

【０１３６】

このように本実施の形態によれば、クライアント装置３の保守インタフェース３０の利用回数（ログイン回数）を管理することができる。従って、クライアント装置３の保守インタフェース３０が一度開放された後、保守インタフェース３０が頻繁にアタックされるのを防ぐことができ、クライアント装置３が輻輳することを防ぐことができる。

【０１３７】

なお、本実施の形態では、サーバ側ローカル保守コンソール２からクライアント装置３に利用者認証情報を設定する指示でログイン可能回数を併せて設定するように指示したが、サーバ側ローカル保守コンソール２からクライアント装置３への利用者認証情報の設定指示と、サーバ側ローカル保守コンソール２からクライ

アント装置３へのログイン可能回数の設定指示とを独立させるようにしても良い。また、サーバ側ローカル保守コンソール２からクライアント装置３へのログイン可能回数の設定機能を無くし、ログイン回数管理部３９に予め記憶された固定のログイン可能回数を使用するようにしても良い。

【０１３８】

また、本実施の形態において、第１の実施の形態と同様にそれぞれのクライアント装置３に図１のクライアント側ローカル保守コンソール４を接続し、クライアント装置３内にローカル要求処理部３４を設けるようにしても良い。さらに、利用者認証情報を暗号化せずにサーバ装置１からクライアント装置３へ転送するようにしても良く、その場合には暗号化部１３および復号化部３６は省略される。また、利用者認証情報の再設定時にログイン中の遠隔保守コンソール５を強制切断しないようにしても良く、その場合には強制切断部３７は省略される。さらに、利用可能時間を管理しないようにしても良く、その場合には利用時間管理部３８は省略される。

【０１３９】

【発明の第７の実施の形態】

図３０を参照すると、本発明の第７の実施の形態にかかるクライアント・サーバ型システムは、図２５に示した第６の実施の形態にかかるクライアント・サーバ型システムにおける各クライアント装置３に、利用可能時間基準値３Ａ－１およびログイン可能回数基準値３Ａ－２を予め記憶する手段を備え、遠隔保守コンソール５からの利用者認証情報設定指示中に利用可能時間、ログイン可能回数が含まれていないか、含まれていても受信不良等で使用できない場合に、利用可能時間基準値３Ａ－１およびログイン可能回数基準値３Ａ－２を利用時間管理部３８およびログイン回数管理部３９に設定するようにした点で、第６の実施の形態と相違し、その他は第６の実施の形態と同じである。

【０１４０】

図３１はサーバ側ローカル保守コンソール２から利用者認証情報設定要求が入力された際のサーバ装置１の処理例を示すフローチャートである。システム管理者等は、利用者認証情報の設定対象となるクライアント装置３の指定情報と、設定

したい利用者認証情報としてのユーザ名およびパスワードと、設定したい利用可能時間と、設定したいログイン可能回数とを指定した利用者認証情報設定要求をサーバ側ローカル保守コンソール２から入力する。本実施の形態の場合、利用可能時間およびログイン可能回数の指定は任意であり、クライアント装置３の利用可能時間基準値３Ａ－１、ログイン可能回数基準値３Ａ－２を利用する場合には指定する必要はない。サーバ側ローカル保守コンソール２からの上記要求は、要求受付部１１で受信され（Ｓ７０１）、以下、図２６のステップＳ６０２～Ｓ６１１と同様な処理が行われる（Ｓ７０２～Ｓ７１１）。

【０１４１】

図３２はサーバ装置１から利用者認証情報設定指示がＬＡＮ６経由で送信されてきた際のクライアント装置３の処理例を示すフローチャートであり、図２７のステップＳ５２１、Ｓ５２２、Ｓ６２１、Ｓ６２２の部分がステップＳ７０１～Ｓ７０８に置き換えられている点が図２７のフローチャートと相違する。ＬＡＮ経由で利用者認証情報設定指示が送信されてきたクライアント装置３は、この指示をリモート要求処理部３３で受信すると（Ｓ１２１）、この指示中の暗号化されたユーザ名およびパスワードを復号化部３６で復号化し（Ｓ３１１～Ｓ３１３）、ユーザ名およびパスワードについて、また若し含まれていれば利用可能時間およびログイン可能回数について、所定の桁数を満たすかどうか等のチェックを行う（Ｓ１２２）。利用可能時間が含まれており利用可能ならば（Ｓ７０１でＹＥＳ）、それを利用時間管理部３８に伝達し（Ｓ７０２）、利用可能時間が含まれていないか或いは受信不良で使えない場合には（Ｓ７０１でＮＯ）、利用可能時間基準値３Ａ－１を利用時間管理部３８に伝達する（Ｓ７０３）。利用時間管理部３８はこの伝達された利用可能時間を記憶する（Ｓ７０４）。さらに、リモート要求処理部３３は、ログイン可能回数が指示中に含まれており利用可能ならば（Ｓ７０５でＹＥＳ）、それをログイン回数管理部３９に伝達し（Ｓ７０６）、ログイン可能回数が含まれていないか或いは受信不良で使えない場合には（Ｓ７０５でＮＯ）、ログイン可能回数基準値３Ａ－２をログイン回数管理部３９に伝達する（Ｓ７０７）。ログイン回数管理部３９はこの伝達されたログイン可能回数を記憶する（Ｓ７０８）。以降、図２７の場合と同様な処理が行われる（Ｓ１

２３、Ｓ４０１～Ｓ４０５、Ｓ１２４、Ｓ１２５、Ｓ５２３）。

【０１４２】

本実施の形態によれば、サーバ側ローカル保守コンソール２からクライアント装置３に利用者認証情報を設定して保守インタフェース３０を開放するに際し、サーバ側ローカル保守コンソール２から利用可能時間が設定されない場合にも、クライアント装置３の利用可能時間基準値３Ａ－１を用いて利用時間を管理でき、利用可能時間基準値３Ａ－１を超えた場合に保守インタフェース３０の利用を強制的に禁止することができる。従って、利用可能時間が指定されずにクライアント装置３の保守インタフェース３０が開放された場合も、保守インタフェース３０が長時間開放し続け、悪意のアクセスの危険性が高くなることを防ぐことができる。

【０１４３】

また本実施の形態によれば、サーバ側ローカル保守コンソール２からクライアント装置３に利用者認証情報を設定して保守インタフェース３０を開放するに際し、サーバ側ローカル保守コンソール２からログイン可能回数が設定されない場合にも、クライアント装置３のログイン可能回数基準値３Ａ－２を用いてログイン回数を管理でき、ログイン回数がログイン可能回数基準値３Ａ－２を超えた場合に保守インタフェース３０の利用を強制的に禁止することができる。従って、ログイン可能回数が指定されずにクライアント装置３の保守インタフェース３０が開放された場合にも、保守インタフェース３０が多数回アタックされるのを防ぐことができる。

【０１４４】

なお、本実施の形態において、第１の実施の形態と同様にそれぞれのクライアント装置３に図１のクライアント側ローカル保守コンソール４を接続し、クライアント装置３内にローカル要求処理部３４を設けるようにしても良い。また、利用者認証情報を暗号化せずにサーバ装置１からクライアント装置３へ転送するようにしても良く、その場合には暗号化部１３および復号化部３６は省略される。さらに、利用者認証情報の再設定時にログイン中の遠隔保守コンソール５を強制切断しないようにしても良く、その場合には強制切断部３７は省略される。

【０１４５】

【発明の第８の実施の形態】

図３３を参照すると、本発明の第８の実施の形態にかかるクライアント・サーバ型システムは、図３０に示した第７の実施の形態にかかるクライアント・サーバ型システムにおける各クライアント装置３に、保守インタフェース３０を開放してからの初回のログインに限り、利用時間管理部３８における残り利用時間を予め定められた延長時間だけ延長する利用時間延長部３Ｂを備えている点で、第７の実施の形態と相違し、その他は第７の実施の形態と同じである。

【０１４６】

図３４（Ａ）は利用時間延長部３Ｂの処理例を示すフローチャートである。利用時間延長部３Ｂは、たとえば利用時間管理部３８と同時に起動される。利用時間管理部３８は、先ず、利用者認証部３２に利用者認証情報が設定されることで保守インタフェース３０が開放されてから、初めて遠隔保守コンソール５のログインが行われたかどうかを検出する（Ｓ８０１）。これは、例えばログイン回数管理部３４で管理されているログイン回数が１になったかどうかを検出することで可能である。遠隔保守コンソール５からの初回のログインを検出すると、利用時間延長部３Ｂは、利用時間管理部３８で管理されている利用時間の残り時間が予め設定された時間以下であるかどうかを検出する（Ｓ８０２）。そして、残り利用時間が予め設定された時間以下であれば（Ｓ８０２でＹＥＳ）、利用時間管理部３８で管理されている残り時間情報に、予め定められた延長時間を加算する（Ｓ８０３）。加算せずに延長時間だけを残り時間として再設定しても良い。他方、初回のログイン時点における残り利用時間が予め設定された時間以下でなければ（Ｓ８０２でＮＯ）、もはや利用時間の延長処理を行わないため、図３４（Ａ）の処理を終了する。

【０１４７】

図３５は本実施の形態の動作例を示すシーケンスチャートであり、以下の２つの場面のシーケンスが示されている。

（１）サーバ側ローカル保守コンソール２からクライアント装置３への利用者認証情報および利用可能時間ならびにログイン可能回数の設定

（２）遠隔保守コンソール５からのクライアント装置３への初回のログイン

【０１４８】

（１）のシーケンスにおける本実施の形態の動作は図２９のシーケンスの場合と同じであるので、以下では遠隔保守コンソール５から保守作業者がクライアント装置３へ初めてログインした場面（２）の動作を、図３３～図３５を参照して説明する。

【０１４９】

クライアント装置３の利用者認証部３２にユーザ名およびパスワードが設定され、利用時間管理部３８に利用可能時間が設定され、さらにログイン回数管理部３９にログイン可能回数が設定された後、暫く経って、保守作業者が遠隔保守コンソール５からＬＡＮ６経由でクライアント装置３に対してユーザ名およびパスワードを指定したログイン要求を入力すると（図３５のＲ８０１）、ログイン回数管理部３９でログイン回数が更新され（図３５のＲ８０２）、ログイン回数＝１となる。また利用者認証処理Ｒ８０３が実施され、ログイン要求中のユーザ名およびパスワードが利用者認証部３２に登録されているユーザ名およびパスワードと一致すると、ログインが許可される（図３５のＲ８０４）。これにより、遠隔保守コンソール5からクライアント装置３の保守対象部３１に対するアクセスが可能となる。

【０１５０】

利用者認証部３２に利用者認証情報が設定され保守インタフェース３０が開放されてから遠隔保守コンソールがログインするまでに暫く時間が空いていたため、ログインした時点で利用時間の残り時間が予め定められた時間以下であった場合（図３５のＲ８０５）、そのことが利用時間延長部３Ｂで検出され（図３４（Ａ）のＳ８０２でＹＥＳ）、利用時間管理部３３の残り利用時間に予め定められた延長時間が加算される（図３５のＲ８０６、図３４（Ａ）のＳ８０３）。その後、図３５のシーケンスでは、保守作業者が保守作業を終えたので、遠隔保守コンソール５をログアウトしている（Ｒ８０７～Ｒ８０９）。

【０１５１】

このように本実施の形態によれば、サーバ側ローカル保守コンソール２からクラ

イアント装置３の保守インタフェース３０を時間設定して開放した後、遠隔保守コンソール５からの初回のログインが利用時間終了近くで実行された場合に、十分な保守作業を行わせることを目的として、一定時間の利用時間延長を行うことができる。従って、何らかの理由で初回のログインが遅れた場合でも保守作業を支障なく行うことが可能となる。なお、図３４（Ａ）の処理では、初回のログイン時点における残り利用時間が所定時間以下であった場合に利用時間の延長を認めたが、初回のログイン時点における残り利用時間が所定時間以上あっても、保守作業に時間がかかったため残り利用時間が足りなくなった場合に利用時間を延長するようにしても良い。図３４（Ｂ）はこのような実施の形態における利用時間延長部３Ｂの処理例を示すフローチャートであり、図３４（Ａ）のフローチャートにステップＳ８０４が追加されている。利用時間管理部３８は、利用者認証部３２に利用者認証情報が設定されることで保守インタフェース３０が開放されてから、初めて遠隔保守コンソール５のログインが行われたことを検出すると（Ｓ８０１）、利用時間管理部３８で管理されている利用時間の残り時間が予め設定された時間以下であるかどうか（Ｓ８０２）、初回のログインが継続中であるかどうか（Ｓ８０３）をそれぞれ検出する。初回のログインが継続中であるかどうかはログイン・ログアウト処理部３５で管理されているログイン状態を参照することで検出できる。そして、初回のログイン中に利用時間の残り時間が予め定められた時間以下になっていることを検出すると（Ｓ８０２でＹＥＳ）、利用時間管理部３８で管理されている残り時間情報に、予め定められた延長時間を加算する（Ｓ８０３）。加算せずに延長時間だけを残り時間として再設定しても良い。他方、初回のログインが終了し、遠隔保守コンソール５がログアウトした場合（Ｓ８０４でＮＯ）、もはや利用時間の延長処理を行わないため、図３４（Ｂ）の処理を終了する。

【０１５２】

なお、本実施の形態において、第１の実施の形態と同様にそれぞれのクライアント装置３に図１のクライアント側ローカル保守コンソール４を接続し、クライアント装置３内にローカル要求処理部３４を設けるようにしても良い。さらに、利用者認証情報を暗号化せずにサーバ装置１からクライアント装置３へ転送するよ

うにしても良く、その場合には暗号化部１３および復号化部３６は省略される。また、利用者認証情報の再設定時にログイン中の遠隔保守コンソール５を強制切断しないようにしても良く、その場合には強制切断部３７は省略される。さらに、ログイン可能回数を管理しないようにしても良く、その場合にはログイン回数管理部３９は省略される。この場合、保守インタフェース３０開放後の初回のログインかどうかは、例えば利用時間延長部３Ｂ内で保守インタフェース３０開放後のログイン回数を管理することで可能である。

【０１５３】

【発明の第９の実施の形態】

図３６を参照すると、本発明の第９の実施の形態にかかるクライアント・サーバ型システムは、図３３に示した第８の実施の形態にかかるクライアント・サーバ型システムにおける各クライアント装置３に、ログイン中の遠隔保守コンソール５から保守インタフェース利用終了通知を受信したときに利用者認証部３２に登録されている利用者認証情報を無効化し、利用者認証情報を無効化した旨の通知を遠隔保守コンソール５に送信する認証無効化部３Ｃを備えている点で、第８の実施の形態と相違し、その他は第８の実施の形態と同じである。

【０１５４】

図３７は本実施の形態の動作例を示すシーケンスチャートであり、以下の２つの場面のシーケンスが示されている。

（１）サーバ側ローカル保守コンソール２からクライアント装置３への利用者認証情報および利用可能時間ならびにログイン可能回数の設定

（２）遠隔保守コンソール５からのクライアント装置３へのログインと保守インタフェース利用終了通知の送出

【０１５５】

（１）のシーケンスにおける本実施の形態の動作は図２９のシーケンスの場合と同じであるので、以下では遠隔保守コンソール５から保守作業者がクライアント装置３へログインして保守作業を行い、保守作業の終了時に保守インタフェース利用終了通知を遠隔保守コンソール５から入力した場面（２）の動作を、図３６および図３７を参照して説明する。

【０１５６】

クライアント装置３の利用者認証部３２にユーザ名およびパスワードが設定され、利用時間管理部３８に利用可能時間が設定され、さらにログイン回数管理部３９にログイン可能回数が設定された後、保守作業者が遠隔保守コンソール５からＬＡＮ６経由でクライアント装置３に対してユーザ名およびパスワードを指定したログイン要求を入力すると（図３７のＲ９０１）、ログイン回数管理部３９でログイン回数が更新され（図３７のＲ９０２）、また利用者認証処理Ｒ９０３が実施され、ログイン要求中のユーザ名およびパスワードが利用者認証部３２に登録されているユーザ名およびパスワードと一致すると、ログインが許可される（図３７のＲ９０４）。これにより、遠隔保守コンソール５からクライアント装置３の保守対象部３１に対するアクセスが可能となる。

【０１５７】

保守作業者がクライアント装置３の保守対象部３１に対する保守を終え、遠隔保守コンソール５から保守インタフェース利用終了通知を入力すると（Ｒ９０５）、それがクライアント装置３のログイン・ログアウト処理部３５を通じて認証無効化部３Ｃに伝達される。認証無効化部３Ｃは、利用者認証部３２に対して利用者認証情報の無効化を指示し、利用者認証部３２はそれに応じて、登録されている利用者認証情報を消去する等して無効にする（Ｒ９０６）。その後、認証無効化３Ｃは、遠隔保守コンソール５に対して利用者認証情報無効化通知を送出する（Ｒ９０７）。以後、保守インタフェース３０は再度開放されるまで閉塞され、その利用は不可能となる。

【０１５８】

このように本実施の形態によれば、サーバ側ローカル保守コンソール２からクライアント装置３の保守インタフェース３０を時間設定して開放した後、遠隔保守コンソール５からログインして保守作業を行い、その終了時に遠隔保守コンソール５側から保守インタフェース利用終了通知を入力することにより、利用時間終了前であってもクライアント装置３の保守インタフェース３０を利用禁止とすることができる。このように保守作業終了とともに利用者認証情報を無効化できるようにしたことにより、保守インタフェース３０が長時間開放し続け、悪意のア

クセスの危険性が高くなることを防ぐことができる。

【０１５９】

なお、本実施の形態において、第１の実施の形態と同様にそれぞれのクライアント装置３に図１のクライアント側ローカル保守コンソール４を接続し、クライアント装置３内にローカル要求処理部３４を設けるようにしても良い。さらに、利用者認証情報を暗号化せずにサーバ装置１からクライアント装置３へ転送するようにしても良く、その場合には暗号化部１３および復号化部３６は省略される。また、利用者認証情報の再設定時にログイン中の遠隔保守コンソール５を強制切断しないようにしても良く、その場合には強制切断部３７は省略される。さらに、利用時間を延長しないようにしても良く、その場合には利用時間延長部３Ｂは省略される。また利用可能時間を管理しないようにしても良く、その場合には利用時間管理部３８および利用時間延長部３Ｂは省略される。また、ログイン可能回数を管理しないようにしても良く、その場合にはログイン回数管理部３９は省略される。

【０１６０】

以上本発明の実施の形態について説明したが、本発明は以上の実施の形態にのみ限定されず、その他各種の付加変更が可能である。例えば、サーバ装置１とクライアント装置とを接続するネットワークは、ＬＡＮに限られず、インターネットやイントラネット等の他の種類のネットワークであっても良い。

【０１６１】

本発明のサーバ装置およびクライアント装置は、その有する機能をハードウェア的に実現することは勿論、コンピュータとサーバプログラム、クライアントプログラムとで実現することができる。サーバプログラム、クライアントプログラムは、磁気ディスクや半導体メモリ等のコンピュータ可読記録媒体に記録されて提供され、サーバ装置を構成するコンピュータ、クライアント装置を構成するコンソールの立ち上げ時などにコンピュータに読み取られ、そのコンピュータの動作を制御することにより、そのコンピュータを前述した各実施の形態におけるサーバ装置、クライアント装置として機能させる。

【０１６２】

【発明の効果】

以上説明したように本発明によれば、以下のような効果が得られる。

【０１６３】

クライアント・サーバ型分散システムにおいて複数のクライアント装置の保守インタフェースに対するセキュリティ確保のための利用者認証情報の設定および無効化を、サーバ側コンソールから遠隔で制御でき、セキュリティの確保と保守の容易性を両立させることが可能となる。

【０１６４】

サーバ装置からクライアント装置にネットワークを通じて転送される利用者認証情報を暗号化したため、より強固なセキュリティを実現することができる。

【０１６５】

利用者認証情報がクライアント装置に設定された後これらが有効である時間、即ち、保守インタフェースの利用可能時間を導入し、利用可能時間経過後に自動的に利用者認証情報を無効にすることにより、保守インタフェースが長時間にわたって開放され続け、悪意のアクセスの危険性が高まることを防ぐことができる。特に、サーバ装置から利用可能時間が指定された場合にはそれを使用し、指定されない場合にはクライアント側に記憶されている利用可能時間基準値を使用する構成にあっては、システム管理者の選択によって利用可能時間を自由に決定することができると共に、指定忘れなどの場合があっても保守インタフェースが長時間にわたって開放し続け、悪意のアクセスの危険性が高まるのを防ぐことができる。

【０１６６】

初回のログインに限って利用可能時間の延長を自動的に行うようにしたことにより、セキュリティを確保しつつ、ログインするのが遅れた保守作業者による保守作業を支障なく行わせることができる。

【０１６７】

保守インタフェースが開放されてからのログイン回数が所定のログイン可能回数に達すると、ログイン中のアクセスを停止させ、利用者認証情報を無効化するため、ログイン、ログアウトを頻繁に繰り返す悪意の者からの頻繁なアタックを防

止でき、セキュリティを確保することができる。

【０１６８】

保守作業を終了した保守者から入力された保守インタフェース利用終了通知に連動して、利用者認証情報を自動的に無効化するため、保守インタフェースが長時間にわたって開放され続け、悪意のアクセスの危険性が高まるのを防ぐことができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図２】

本発明の第１の実施の形態におけるサーバ側ローカル保守コンソールから利用者認証情報設定要求が入力された際のサーバ装置の処理例を示すフローチャートである。

【図３】

本発明の第１の実施の形態におけるサーバ側ローカル保守コンソールから利用者認証情報設定無効要求が入力された際のサーバ装置の処理例を示すフローチャートである。

【図４】

本発明の第１の実施の形態におけるサーバ装置から利用者認証情報設定指示がＬＡＮ経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図５】

本発明の第１の実施の形態におけるサーバ装置から利用者認証情報設定無効指示がＬＡＮ経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図６】

本発明の第１の実施の形態におけるクライアント側ローカル保守コンソールから利用者認証情報設定指示が入力された際のクライアント装置の処理例を示すフロ

ーチャートである。

【図７】

本発明の第１の実施の形態におけるクライアント側ローカル保守コンソールから利用者認証情報設定無効要求が入力された際のクライアント装置の処理例を示すフローチャートである。

【図８】

本発明の第１の実施の形態における遠隔保守コンソールからユーザ名およびパスワードの指定を含むログイン要求がＬＡＮ経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図９】

本発明の第１の実施の形態におけるログイン中の遠隔保守コンソールからログアウト要求がＬＡＮ経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図１０】

本発明の第１の実施の形態の動作例を示すシーケンスチャートである。

【図１１】

本発明の第１の実施の形態の動作例を示すシーケンスチャートである。

【図１２】

本発明の第２の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図１３】

本発明の第３の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図１４】

本発明の第３の実施の形態におけるサーバ側ローカル保守コンソールから利用者認証情報設定要求が入力された際のサーバ装置の処理例を示すフローチャートである。

【図１５】

本発明の第３の実施の形態におけるサーバ装置から利用者認証情報設定指示がＬ

ＡＮ経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図１６】

本発明の第３の実施の形態の動作例を示すシーケンスチャートである。

【図１７】

本発明の第４の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図１８】

本発明の第４の実施の形態におけるサーバ装置から利用者認証情報設定指示がＬＡＮ経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図１９】

本発明の第４の実施の形態の動作例を示すシーケンスチャートである。

【図２０】

本発明の第５の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図２１】

本発明の第５の実施の形態におけるサーバ側ローカル保守コンソールから利用者認証情報設定要求が入力された際のサーバ装置の処理例を示すフローチャートである。

【図２２】

本発明の第５の実施の形態におけるサーバ装置から利用者認証情報設定指示がＬＡＮ経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図２３】

本発明の第５の実施の形態における利用時間管理部が利用時間の管理を開始した後の処理例を示すフローチャートである。

【図２４】

本発明の第５の実施の形態の動作例を示すシーケンスチャートである。

【図２５】

本発明の第６の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図２６】

本発明の第６の実施の形態におけるサーバ側ローカル保守コンソールから利用者認証情報設定要求が入力された際のサーバ装置の処理例を示すフローチャートである。

【図２７】

本発明の第６の実施の形態におけるサーバ装置から利用者認証情報設定指示がＬＡＮ経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図２８】

本発明の第６の実施の形態における遠隔保守コンソールからユーザ名およびパスワードの指定を含むログイン要求がＬＡＮ経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図２９】

本発明の第６の実施の形態の動作例を示すシーケンスチャートである。

【図３０】

本発明の第７の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図３１】

本発明の第７の実施の形態におけるサーバ側ローカル保守コンソールから利用者認証情報設定要求が入力された際のサーバ装置の処理例を示すフローチャートである。

【図３２】

本発明の第７の実施の形態におけるサーバ装置から利用者認証情報設定指示がＬＡＮ経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図３３】

本発明の第８の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図３４】

本発明の第８の実施の形態における利用時間延長部の処理例を示すフローチャートである。

【図３５】

本発明の第８の実施の形態の動作例を示すシーケンスチャートである。

【図３６】

本発明の第８の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図３７】

本発明の第９の実施の形態の動作例を示すシーケンスチャートである。

【符号の説明】

１…サーバ装置

１１…要求受付部

１２…要求転送部

１３…暗号化部

２…サーバ装置用のローカル保守コンソール

３…クライアント装置

３１…保守対象部

３２…利用者認証部

３３…リモート要求処理部

３４…ローカル要求処理部

３５…ログイン・ログアウト処理部

３６…復号化部

３７…強制切断部

３８…利用時間管理部

３９…ログイン回数管理部

３Ａ－１…利用可能時間基準値

３Ａ－２…ログイン可能回数基準値

３Ｂ…利用時間延長部

３Ｃ…認証無効化部

４…クライアント装置用のローカル保守コンソール

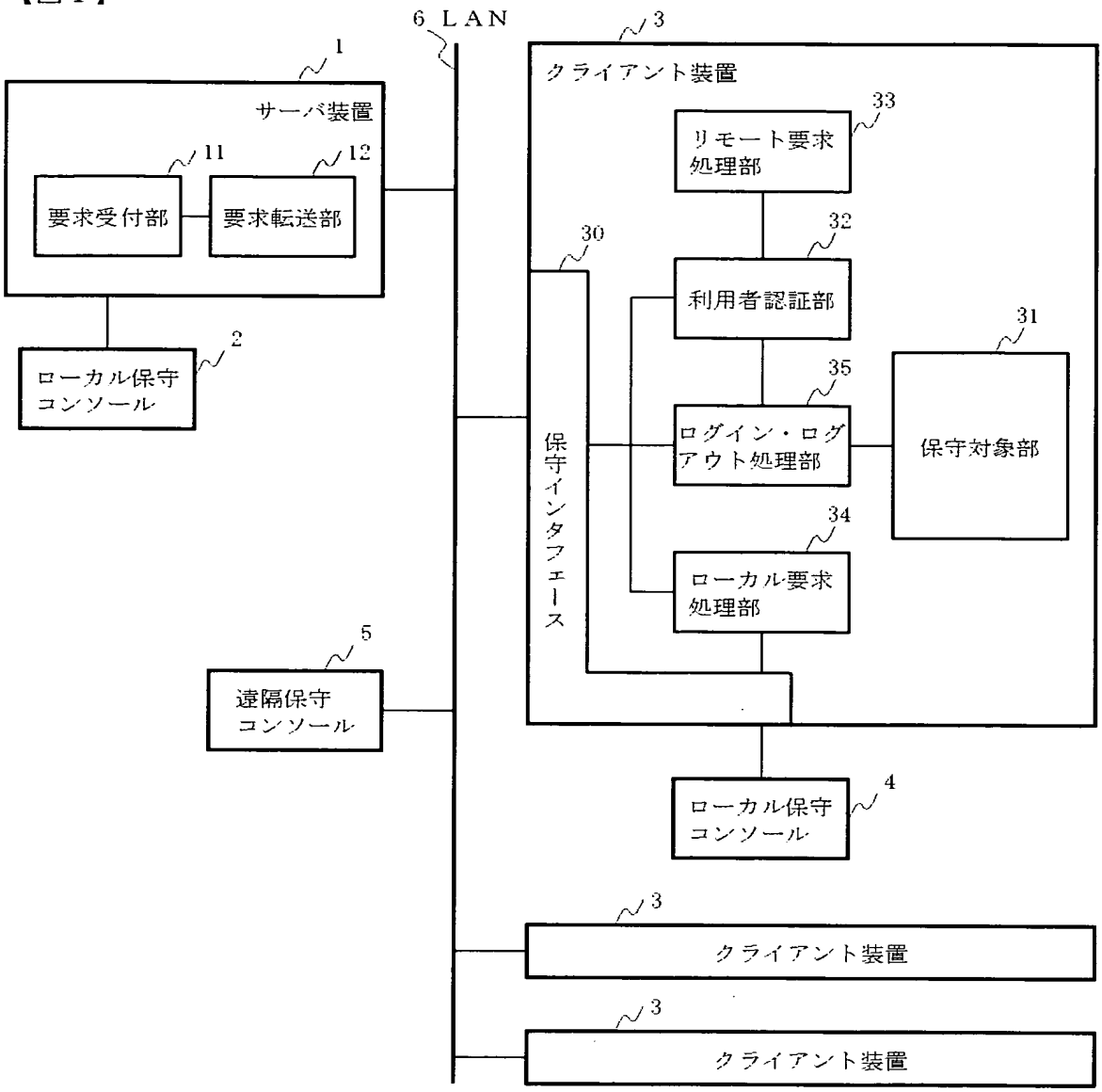
５…遠隔保守コンソール

６…ＬＡＮ

【書類名】　図面

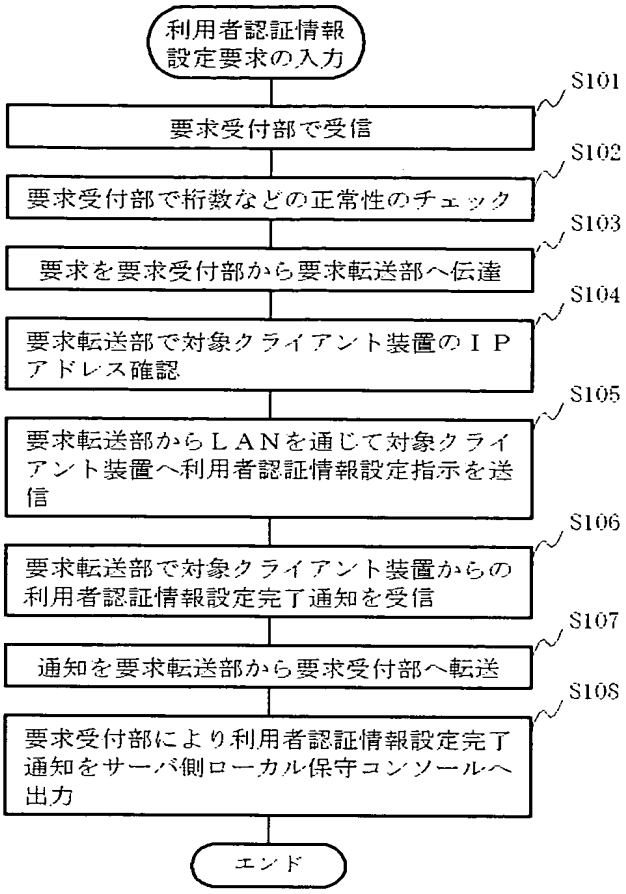
【図１】

【図１】


6 LAN
1
サーバ装置
11
12
要求受付部
要求転送部
2
ローカル保守
コンソール
3
クライアント装置
33
リモート要求
処理部
32
30
利用者認証部
31
35
ログイン・ログ
アウト処理部
保守対象部
保守インタフェース
34
ローカル要求
処理部
5
遠隔保守
コンソール
4
ローカル保守
コンソール
3
クライアント装置
3
クライアント装置

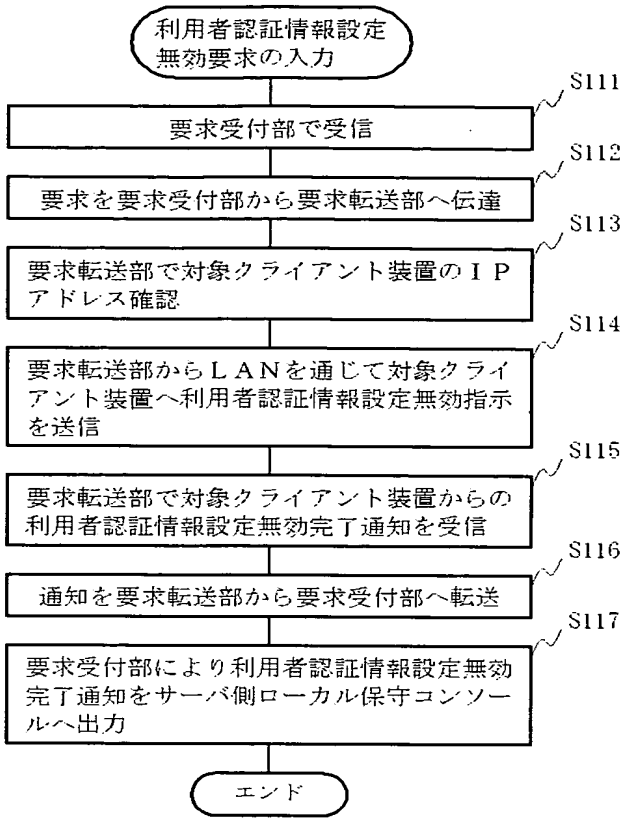
【図２】

【図２】


利用者認証情報設定要求の入力
S101
要求受付部で受信
S102
要求受付部で桁数などの正常性のチェック
S103
要求を要求受付部から要求転送部へ伝達
S104
要求転送部で対象クライアント装置のＩＰアドレス確認
S105
要求転送部からＬＡＮを通じて対象クライアント装置へ利用者認証情報設定指示を送信
S106
要求転送部で対象クライアント装置からの利用者認証情報設定完了通知を受信
S107
通知を要求転送部から要求受付部へ転送
S108
要求受付部により利用者認証情報設定完了通知をサーバ側ローカル保守コンソールへ出力
エンド

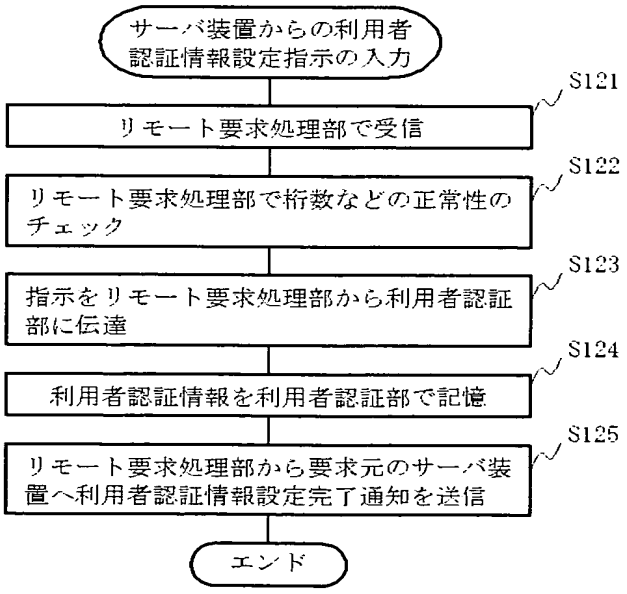
【図３】

【図３】


利用者認証情報設定無効要求の入力
S111
要求受付部で受信
S112
要求を要求受付部から要求転送部へ伝達
S113
要求転送部で対象クライアント装置のＩＰアドレス確認
S114
要求転送部からＬＡＮを通じて対象クライアント装置へ利用者認証情報設定無効指示を送信
S115
要求転送部で対象クライアント装置からの利用者認証情報設定無効完了通知を受信
S116
通知を要求転送部から要求受付部へ転送
S117
要求受付部により利用者認証情報設定無効完了通知をサーバ側ローカル保守コンソールへ出力
エンド

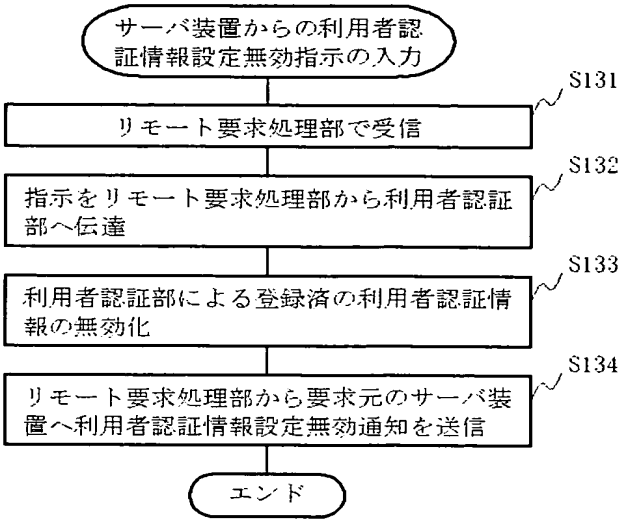
【図４】

【図４】


サーバ装置からの利用者認証情報設定指示の入力
S121
リモート要求処理部で受信
S122
リモート要求処理部で桁数などの正常性のチェック
S123
指示をリモート要求処理部から利用者認証部に伝達
S124
利用者認証情報を利用者認証部で記憶
S125
リモート要求処理部から要求元のサーバ装置へ利用者認証情報設定完了通知を送信
エンド

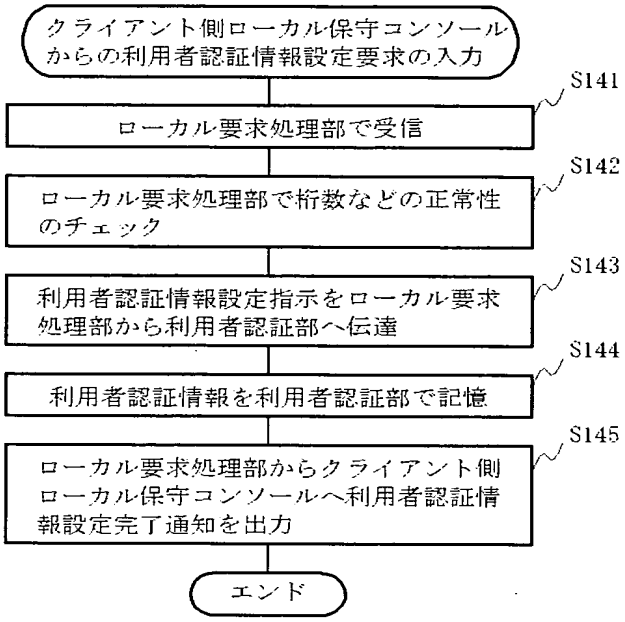
【図５】

【図５】


サーバ装置からの利用者認証情報設定無効指示の入力
S131
リモート要求処理部で受信
S132
指示をリモート要求処理部から利用者認証部へ伝達
S133
利用者認証部による登録済の利用者認証情報の無効化
S134
リモート要求処理部から要求元のサーバ装置へ利用者認証情報設定無効通知を送信
エンド

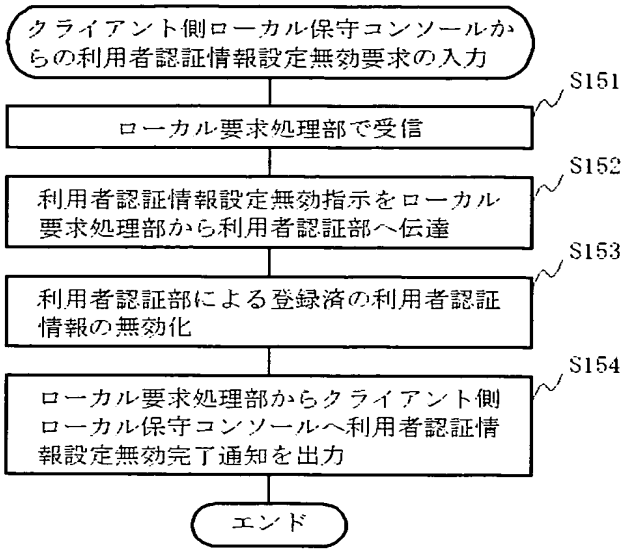
【図６】

【図６】


クライアント側ローカル保守コンソールからの利用者認証情報設定要求の入力
S141
ローカル要求処理部で受信
S142
ローカル要求処理部で桁数などの正常性のチェック
S143
利用者認証情報設定指示をローカル要求処理部から利用者認証部へ伝達
S144
利用者認証情報を利用者認証部で記憶
S145
ローカル要求処理部からクライアント側ローカル保守コンソールへ利用者認証情報設定完了通知を出力
エンド

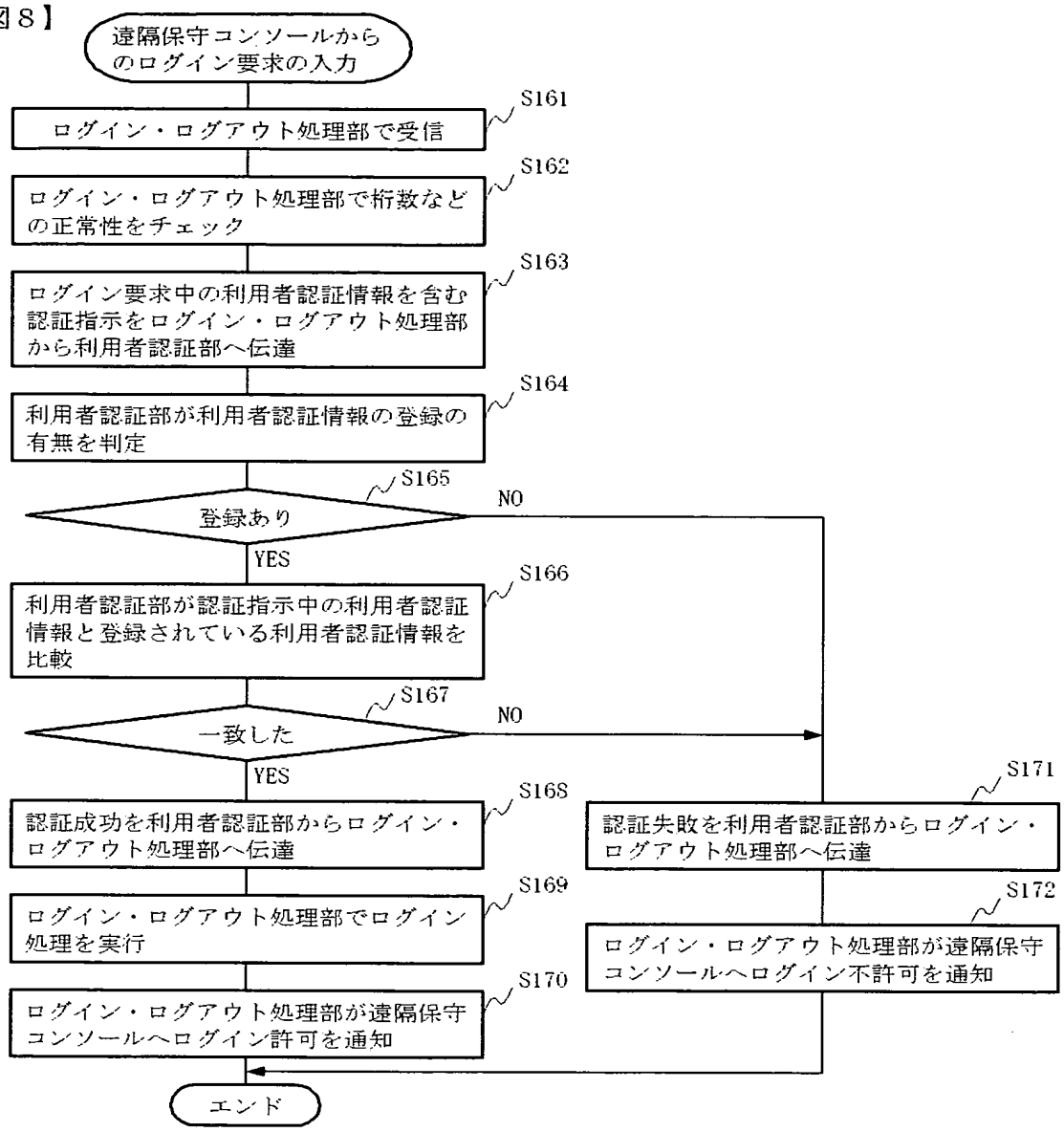
【図７】

【図７】


クライアント側ローカル保守コンソールからの利用者認証情報設定無効要求の入力
S151
ローカル要求処理部で受信
S152
利用者認証情報設定無効指示をローカル要求処理部から利用者認証部へ伝達
S153
利用者認証部による登録済の利用者認証情報の無効化
S154
ローカル要求処理部からクライアント側ローカル保守コンソールへ利用者認証情報設定無効完了通知を出力
エンド

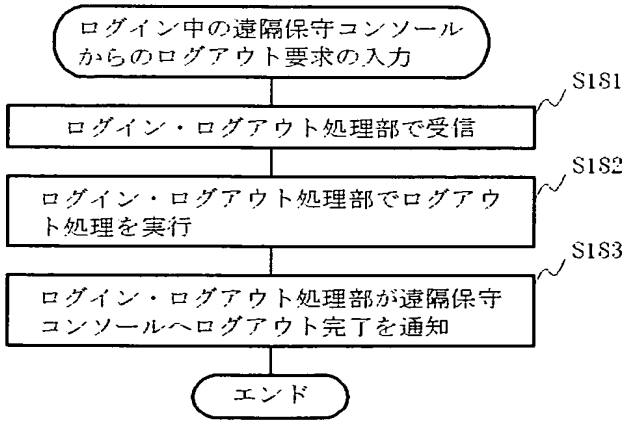
【図８】

【図８】


遠隔保守コンソールからのログイン要求の入力
S161
ログイン・ログアウト処理部で受信
S162
ログイン・ログアウト処理部で桁数などの正常性をチェック
S163
ログイン要求中の利用者認証情報を含む認証指示をログイン・ログアウト処理部から利用者認証部へ伝達
S164
利用者認証部が利用者認証情報の登録の有無を判定
S165
登録あり
NO
YES
S166
利用者認証部が認証指示中の利用者認証情報と登録されている利用者認証情報を比較
S167
一致した
NO
YES
S168
認証成功を利用者認証部からログイン・ログアウト処理部へ伝達
S169
ログイン・ログアウト処理部でログイン処理を実行
S170
ログイン・ログアウト処理部が遠隔保守コンソールへログイン許可を通知
S171
認証失敗を利用者認証部からログイン・ログアウト処理部へ伝達
S172
ログイン・ログアウト処理部が遠隔保守コンソールへログイン不許可を通知
エンド

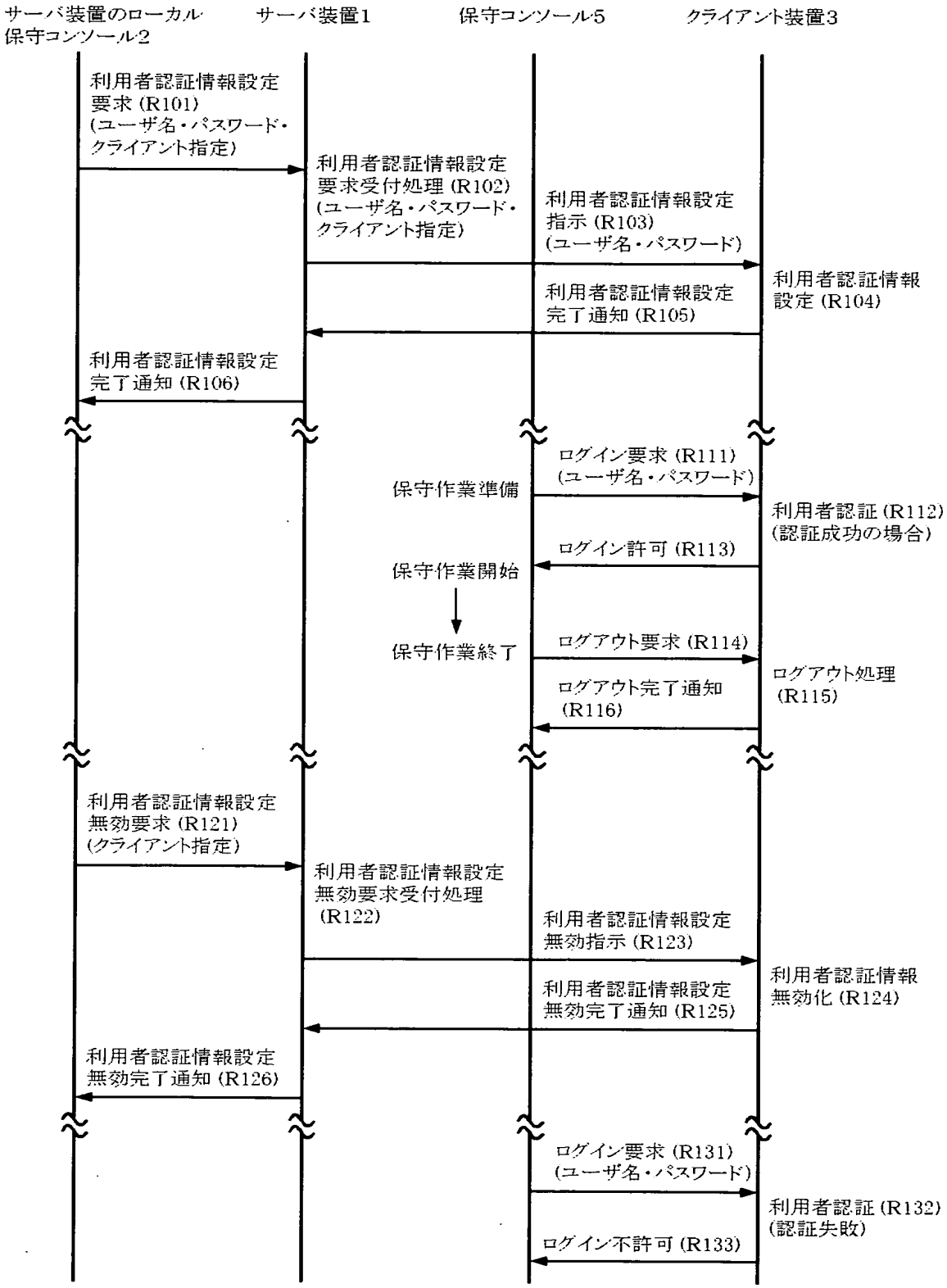
【図９】

【図９】


ログイン中の遠隔保守コンソールからのログアウト要求の入力
S181
ログイン・ログアウト処理部で受信
S182
ログイン・ログアウト処理部でログアウト処理を実行
S183
ログイン・ログアウト処理部が遠隔保守コンソールへログアウト完了を通知
エンド

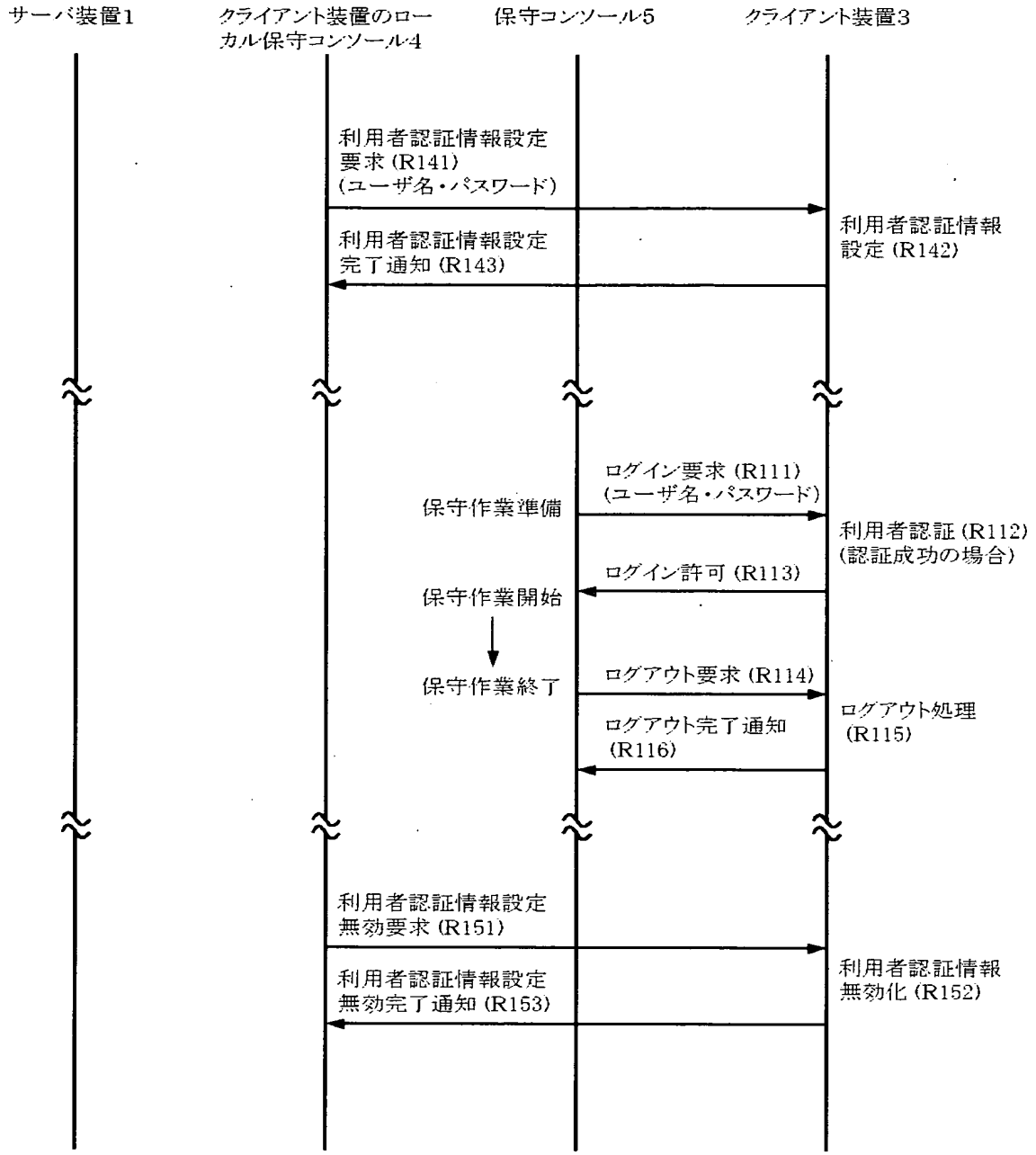
【図１０】

【図１０】


サーバ装置のローカル保守コンソール2
サーバ装置1
保守コンソール5
クライアント装置3
利用者認証情報設定要求 (R101) (ユーザ名・パスワード・クライアント指定)
利用者認証情報設定要求受付処理 (R102) (ユーザ名・パスワード・クライアント指定)
利用者認証情報設定指示 (R103) (ユーザ名・パスワード)
利用者認証情報設定 (R104)
利用者認証情報設定完了通知 (R105)
利用者認証情報設定完了通知 (R106)
ログイン要求 (R111) (ユーザ名・パスワード)
保守作業準備
利用者認証 (R112) (認証成功の場合)
ログイン許可 (R113)
保守作業開始
保守作業終了
ログアウト要求 (R114)
ログアウト処理 (R115)
ログアウト完了通知 (R116)
利用者認証情報設定無効要求 (R121) (クライアント指定)
利用者認証情報設定無効要求受付処理 (R122)
利用者認証情報設定無効指示 (R123)
利用者認証情報無効化 (R124)
利用者認証情報設定無効完了通知 (R125)
利用者認証情報設定無効完了通知 (R126)
ログイン要求 (R131) (ユーザ名・パスワード)
利用者認証 (R132) (認証失敗)
ログイン不許可 (R133)

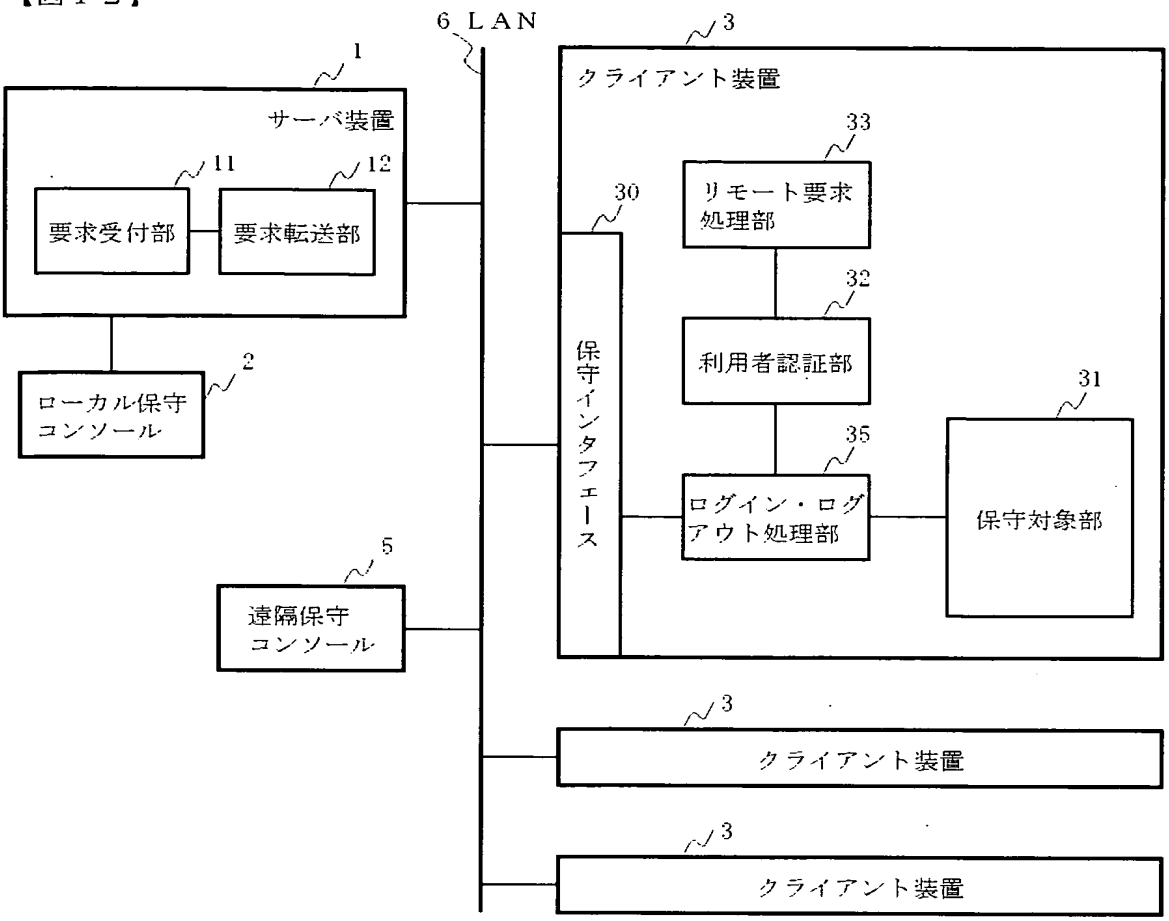
【図１１】

【図１１】


サーバ装置1
クライアント装置のローカル保守コンソール4
保守コンソール5
クライアント装置3
利用者認証情報設定要求 (R141)
(ユーザ名・パスワード)
利用者認証情報設定
利用者認証情報設定完了通知 (R143)
設定 (R142)
ログイン要求 (R111)
(ユーザ名・パスワード)
保守作業準備
利用者認証 (R112)
(認証成功の場合)
ログイン許可 (R113)
保守作業開始
保守作業終了
ログアウト要求 (R114)
ログアウト処理
(R115)
ログアウト完了通知
(R116)
利用者認証情報設定無効要求 (R151)
利用者認証情報
利用者認証情報設定無効完了通知 (R153)
無効化 (R152)

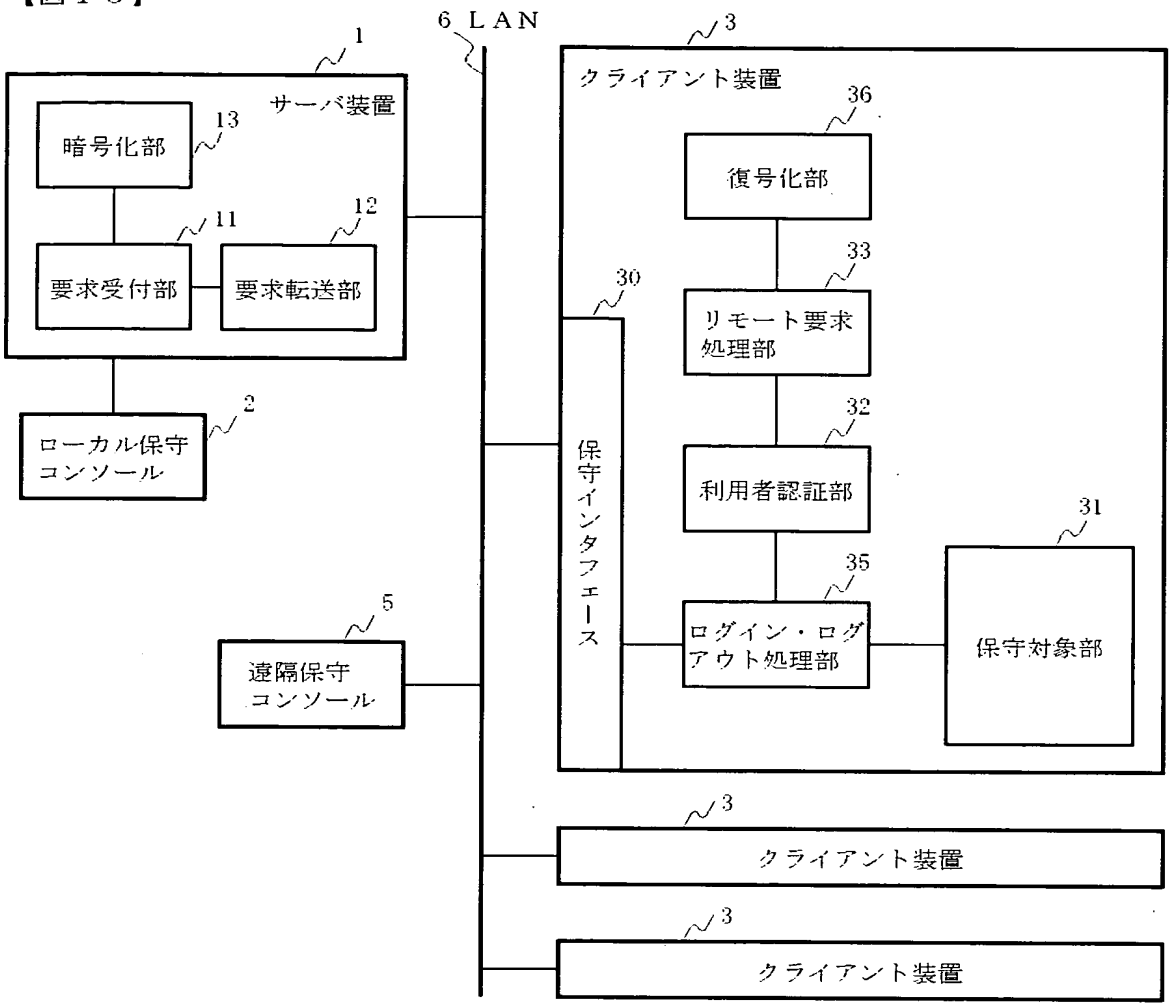
【図１２】

【図１２】


6 LAN
1
サーバ装置
11
12
要求受付部
要求転送部
2
ローカル保守
コンソール
5
遠隔保守
コンソール
3
クライアント装置
33
リモート要求
処理部
30
32
利用者認証部
保守インタフェース
31
35
ログイン・ログ
アウト処理部
保守対象部
3
クライアント装置
3
クライアント装置

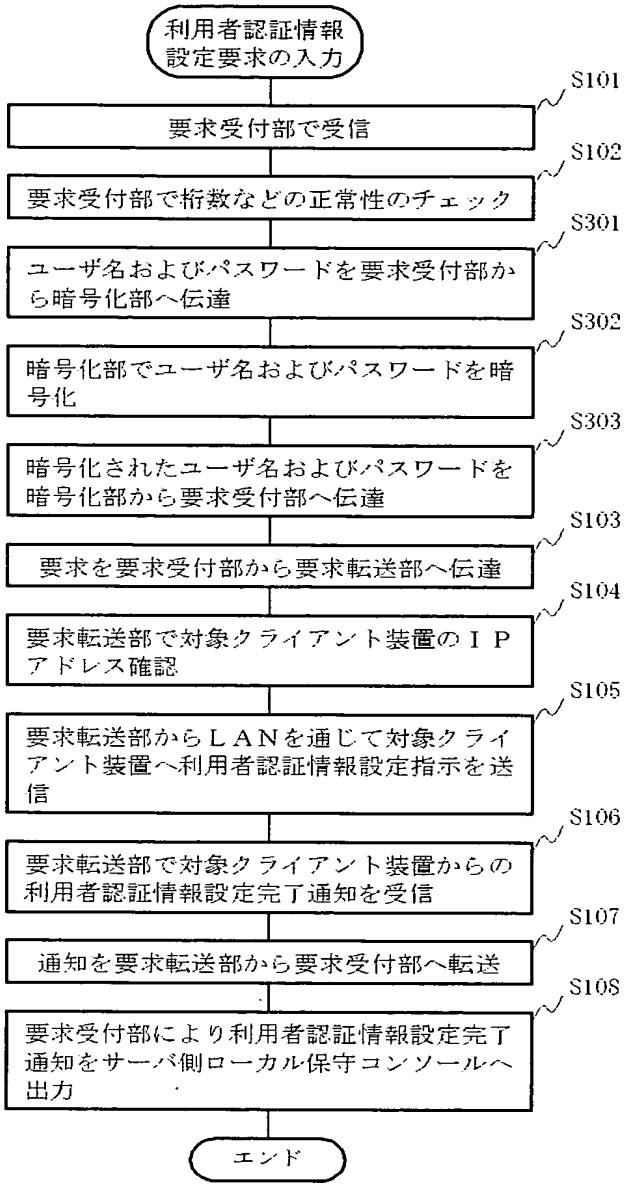
【図１３】

【図１３】


6 LAN
1
サーバ装置
暗号化部
13
11
12
要求受付部
要求転送部
2
ローカル保守
コンソール
5
遠隔保守
コンソール
3
クライアント装置
36
復号化部
33
リモート要求
処理部
30
32
利用者認証部
保守インタフェース
31
35
ログイン・ログ
アウト処理部
保守対象部
3
クライアント装置
3
クライアント装置

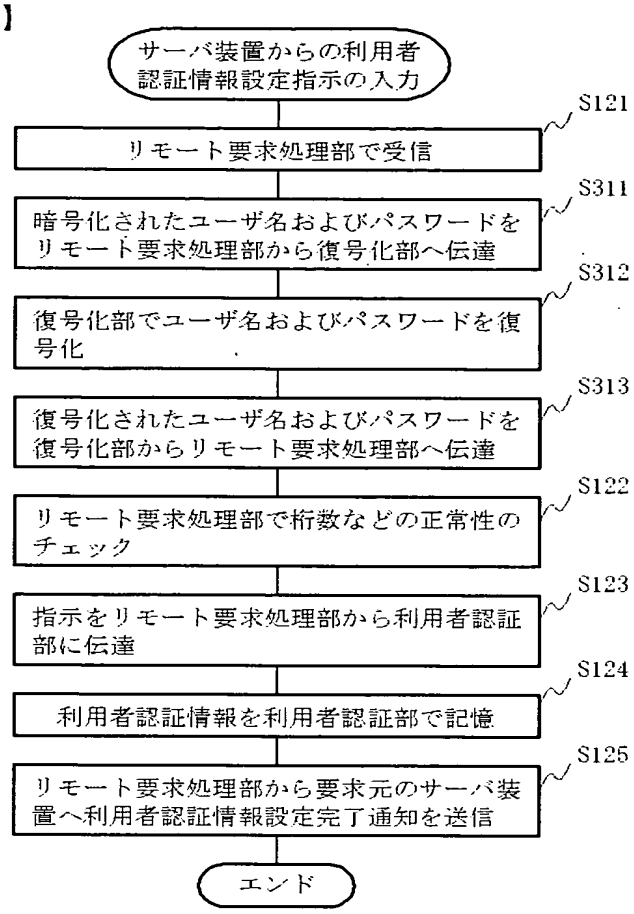
【図１４】

【図１４】


利用者認証情報設定要求の入力
S101
要求受付部で受信
S102
要求受付部で桁数などの正常性のチェック
S301
ユーザ名およびパスワードを要求受付部から暗号化部へ伝達
S302
暗号化部でユーザ名およびパスワードを暗号化
S303
暗号化されたユーザ名およびパスワードを暗号化部から要求受付部へ伝達
S103
要求を要求受付部から要求転送部へ伝達
S104
要求転送部で対象クライアント装置のＩＰアドレス確認
S105
要求転送部からＬＡＮを通じて対象クライアント装置へ利用者認証情報設定指示を送信
S106
要求転送部で対象クライアント装置からの利用者認証情報設定完了通知を受信
S107
通知を要求転送部から要求受付部へ転送
S108
要求受付部により利用者認証情報設定完了通知をサーバ側ローカル保守コンソールへ出力
エンド

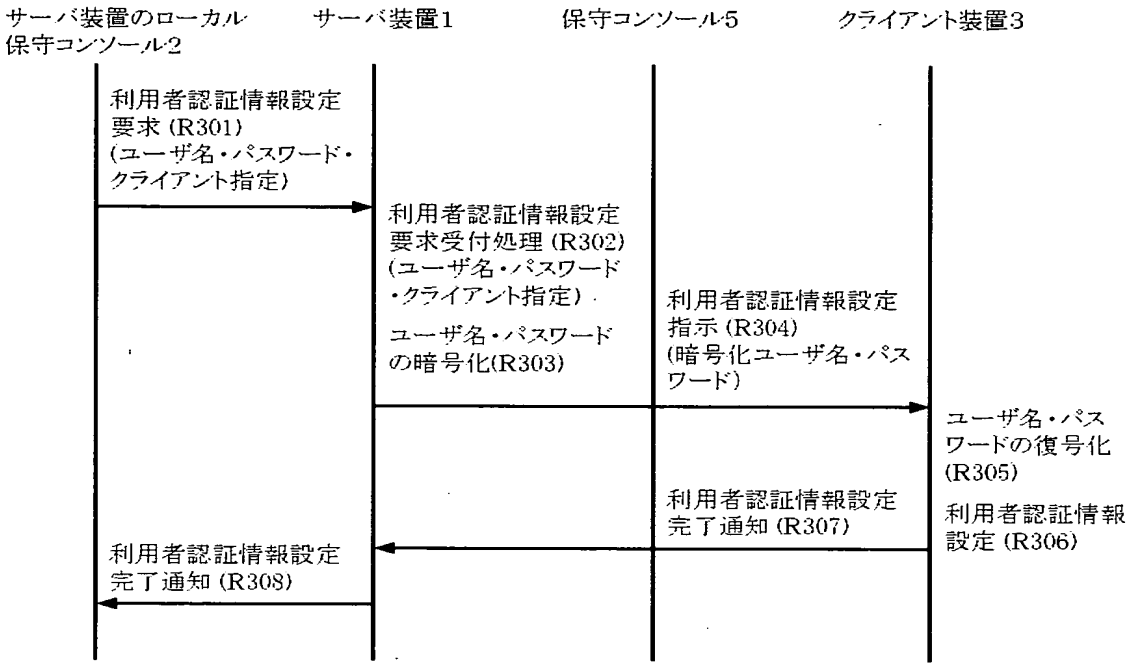
【図１５】

【図１５】


サーバ装置からの利用者認証情報設定指示の入力
S121
リモート要求処理部で受信
S311
暗号化されたユーザ名およびパスワードをリモート要求処理部から復号化部へ伝達
S312
復号化部でユーザ名およびパスワードを復号化
S313
復号化されたユーザ名およびパスワードを復号化部からリモート要求処理部へ伝達
S122
リモート要求処理部で桁数などの正常性のチェック
S123
指示をリモート要求処理部から利用者認証部に伝達
S124
利用者認証情報を利用者認証部で記憶
S125
リモート要求処理部から要求元のサーバ装置へ利用者認証情報設定完了通知を送信
エンド

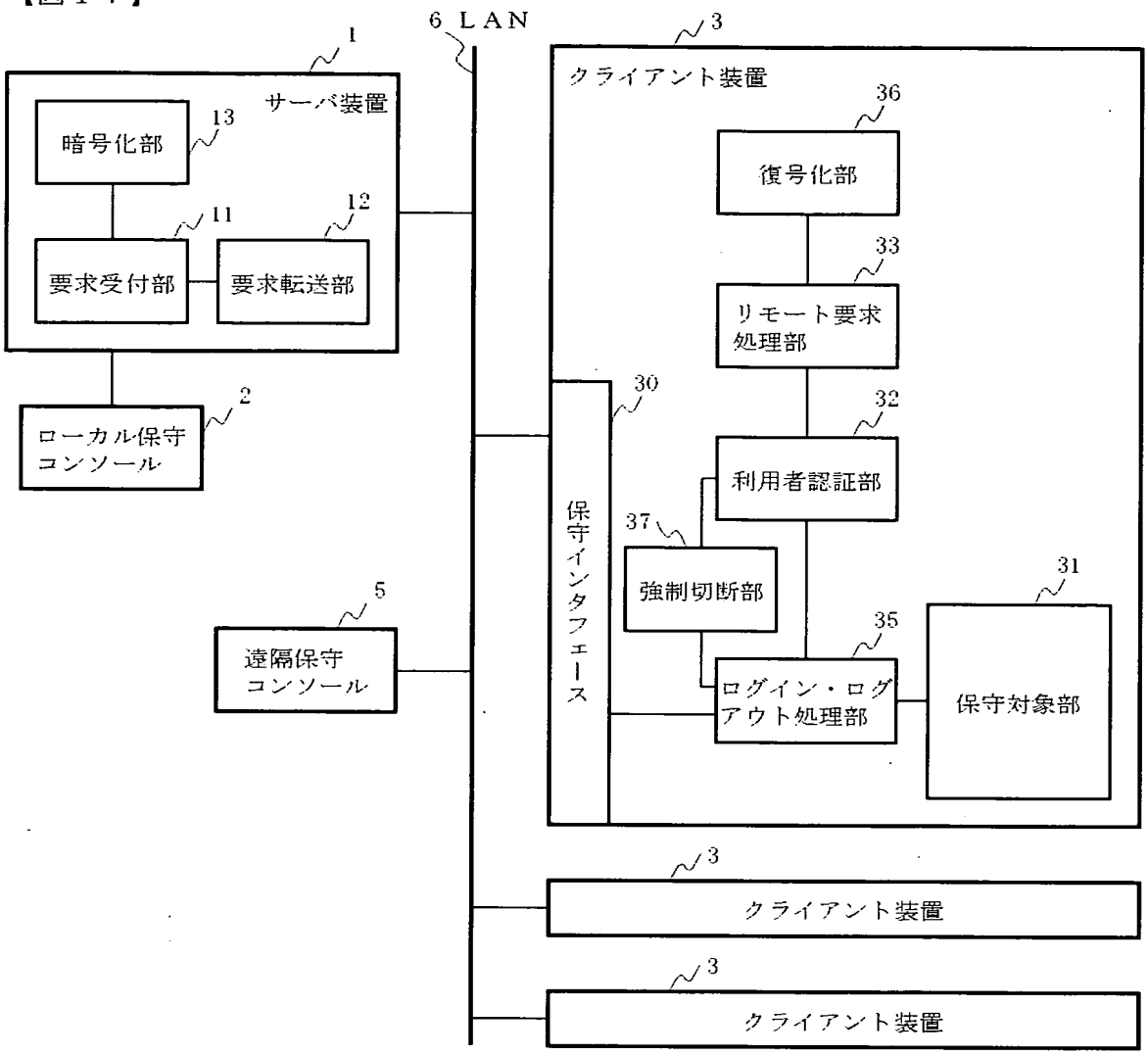
【図１６】

【図１６】


サーバ装置のローカル保守コンソール2
サーバ装置1
保守コンソール5
クライアント装置3
利用者認証情報設定要求 (R301) (ユーザ名・パスワード・クライアント指定)
利用者認証情報設定要求受付処理 (R302) (ユーザ名・パスワード・クライアント指定)
ユーザ名・パスワードの暗号化(R303)
利用者認証情報設定指示 (R304) (暗号化ユーザ名・パスワード)
ユーザ名・パスワードの復号化 (R305)
利用者認証情報設定 (R306)
利用者認証情報設定完了通知 (R307)
利用者認証情報設定完了通知 (R308)

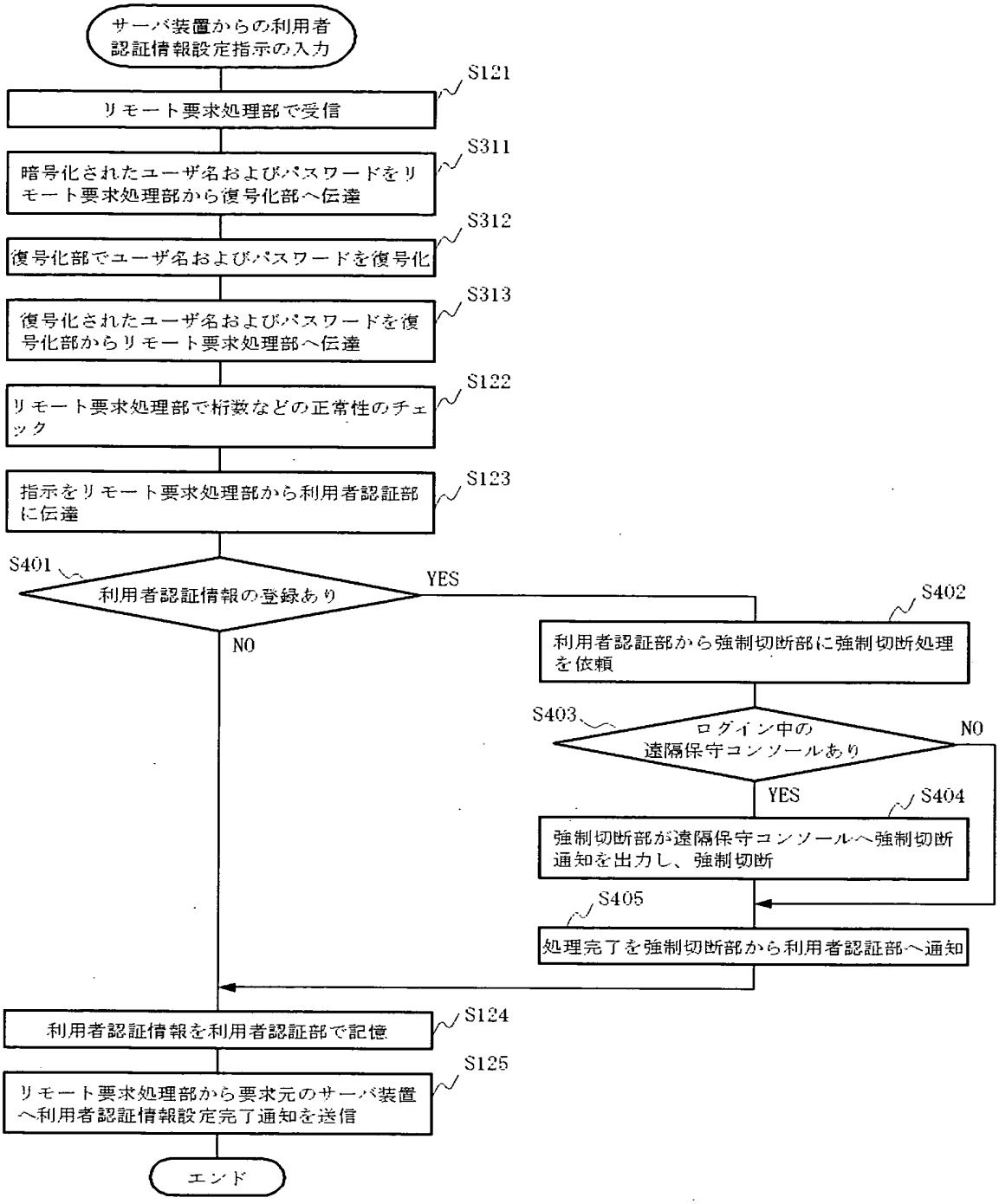
【図１７】

【図１７】


6 LAN
1
サーバ装置
暗号化部
13
11
12
要求受付部
要求転送部
2
ローカル保守
コンソール
5
遠隔保守
コンソール
3
クライアント装置
36
復号化部
33
リモート要求
処理部
30
32
保守インタフェース
利用者認証部
37
強制切断部
31
35
ログイン・ログ
アウト処理部
保守対象部
3
クライアント装置
3
クライアント装置

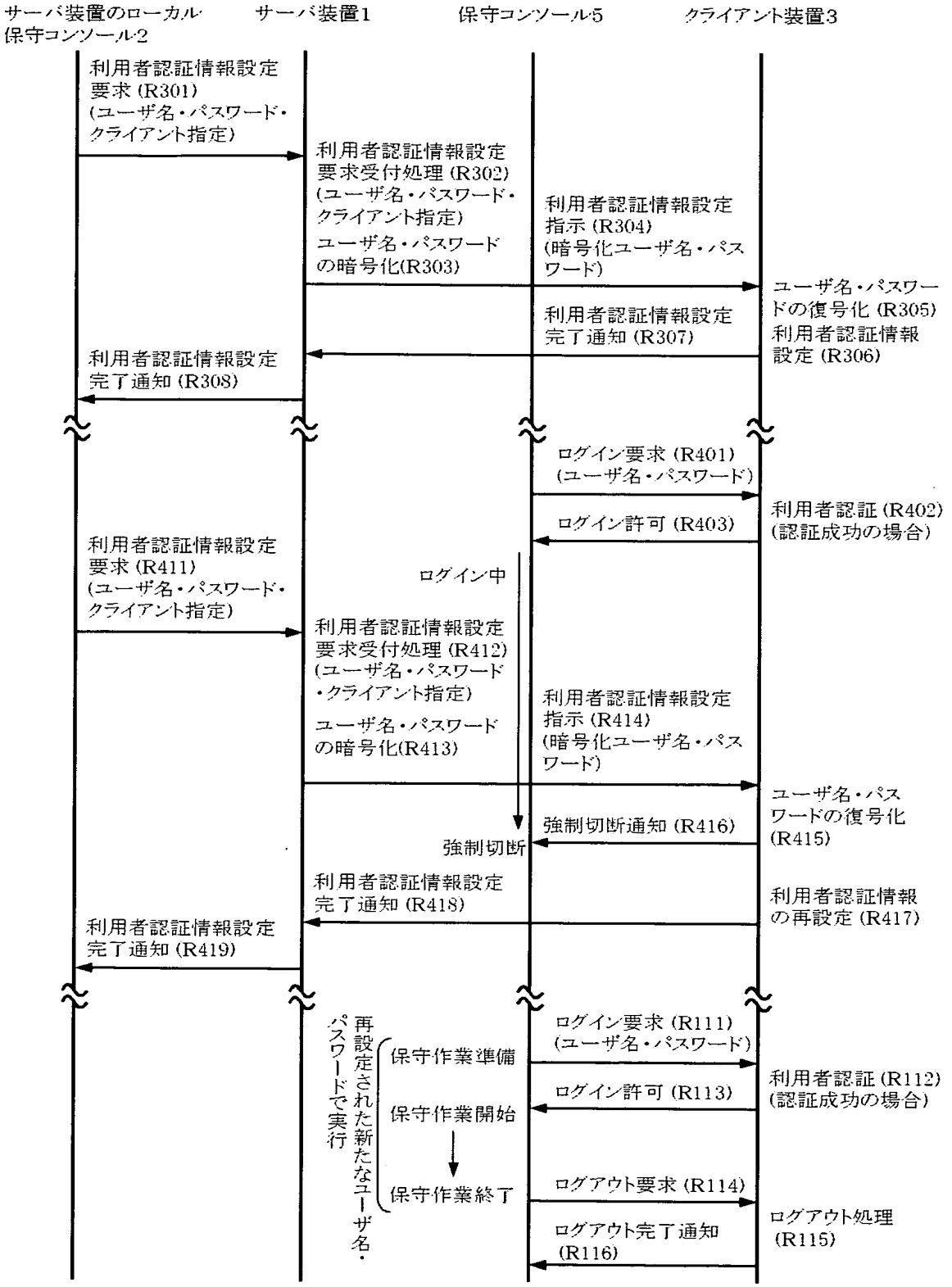
【図１８】

【図１８】


サーバ装置からの利用者認証情報設定指示の入力
S121
リモート要求処理部で受信
S311
暗号化されたユーザ名およびパスワードをリモート要求処理部から復号化部へ伝達
S312
復号化部でユーザ名およびパスワードを復号化
S313
復号化されたユーザ名およびパスワードを復号化部からリモート要求処理部へ伝達
S122
リモート要求処理部で桁数などの正常性のチェック
S123
指示をリモート要求処理部から利用者認証部に伝達
S401
利用者認証情報の登録あり
YES
NO
S402
利用者認証部から強制切断部に強制切断処理を依頼
S403
ログイン中の遠隔保守コンソールあり
NO
YES
S404
強制切断部が遠隔保守コンソールへ強制切断通知を出力し、強制切断
S405
処理完了を強制切断部から利用者認証部へ通知
S124
利用者認証情報を利用者認証部で記憶
S125
リモート要求処理部から要求元のサーバ装置へ利用者認証情報設定完了通知を送信
エンド

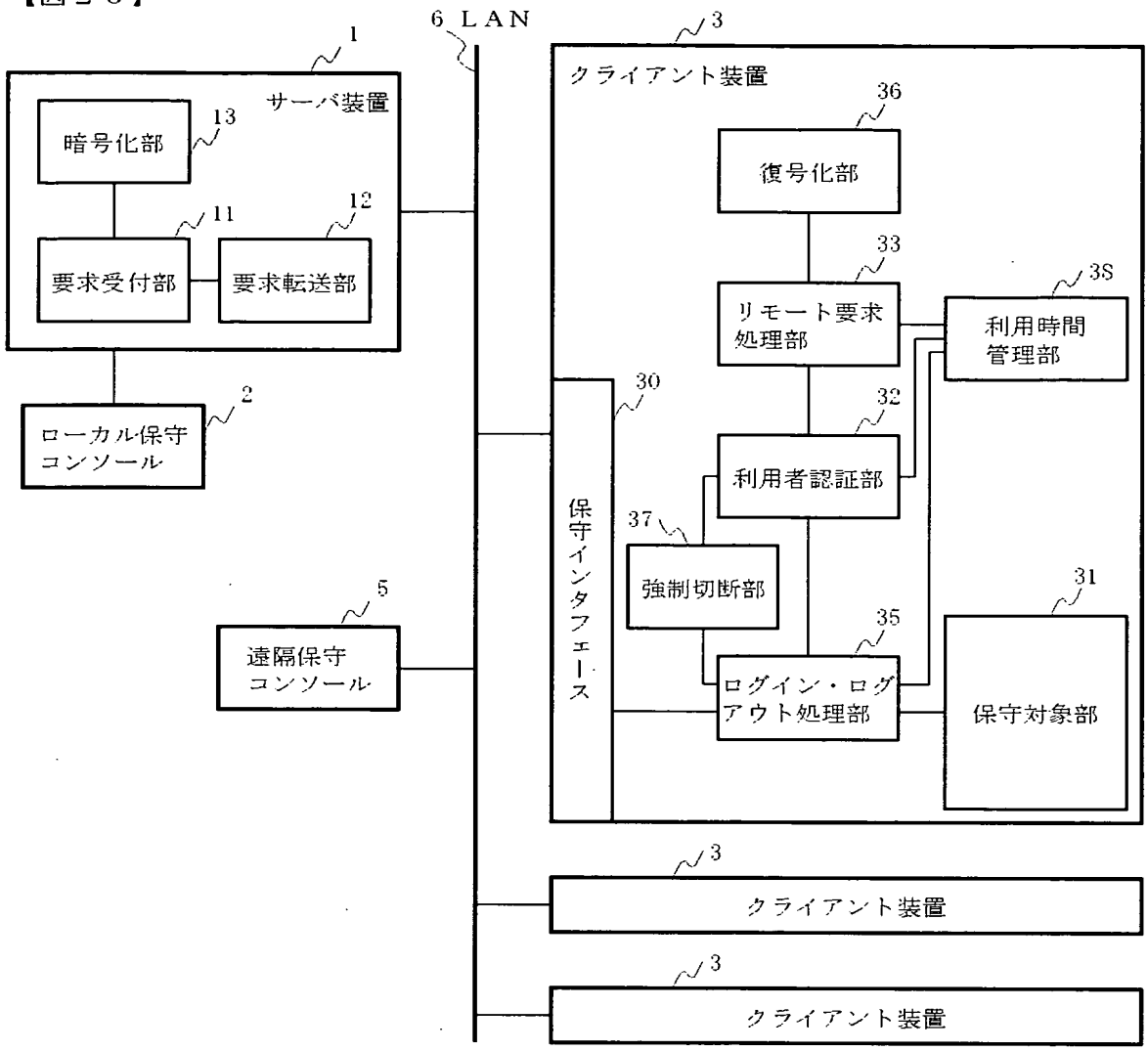
【図１９】

【図１９】


サーバ装置のローカル保守コンソール2
サーバ装置1
保守コンソール5
クライアント装置3
利用者認証情報設定要求 (R301) (ユーザ名・パスワード・クライアント指定)
利用者認証情報設定要求受付処理 (R302) (ユーザ名・パスワード・クライアント指定)
ユーザ名・パスワードの暗号化(R303)
利用者認証情報設定指示 (R304) (暗号化ユーザ名・パスワード)
ユーザ名・パスワードの復号化 (R305)
利用者認証情報設定 (R306)
利用者認証情報設定完了通知 (R307)
利用者認証情報設定完了通知 (R308)
ログイン要求 (R401) (ユーザ名・パスワード)
利用者認証 (R402) (認証成功の場合)
ログイン許可 (R403)
利用者認証情報設定要求 (R411) (ユーザ名・パスワード・クライアント指定)
ログイン中
利用者認証情報設定要求受付処理 (R412) (ユーザ名・パスワード・クライアント指定)
ユーザ名・パスワードの暗号化(R413)
利用者認証情報設定指示 (R414) (暗号化ユーザ名・パスワード)
ユーザ名・パスワードの復号化 (R415)
強制切断通知 (R416)
強制切断
利用者認証情報の再設定 (R417)
利用者認証情報設定完了通知 (R418)
利用者認証情報設定完了通知 (R419)
再設定された新たなユーザ名・パスワードで実行
ログイン要求 (R111) (ユーザ名・パスワード)
保守作業準備
利用者認証 (R112) (認証成功の場合)
ログイン許可 (R113)
保守作業開始
保守作業終了
ログアウト要求 (R114)
ログアウト処理 (R115)
ログアウト完了通知 (R116)

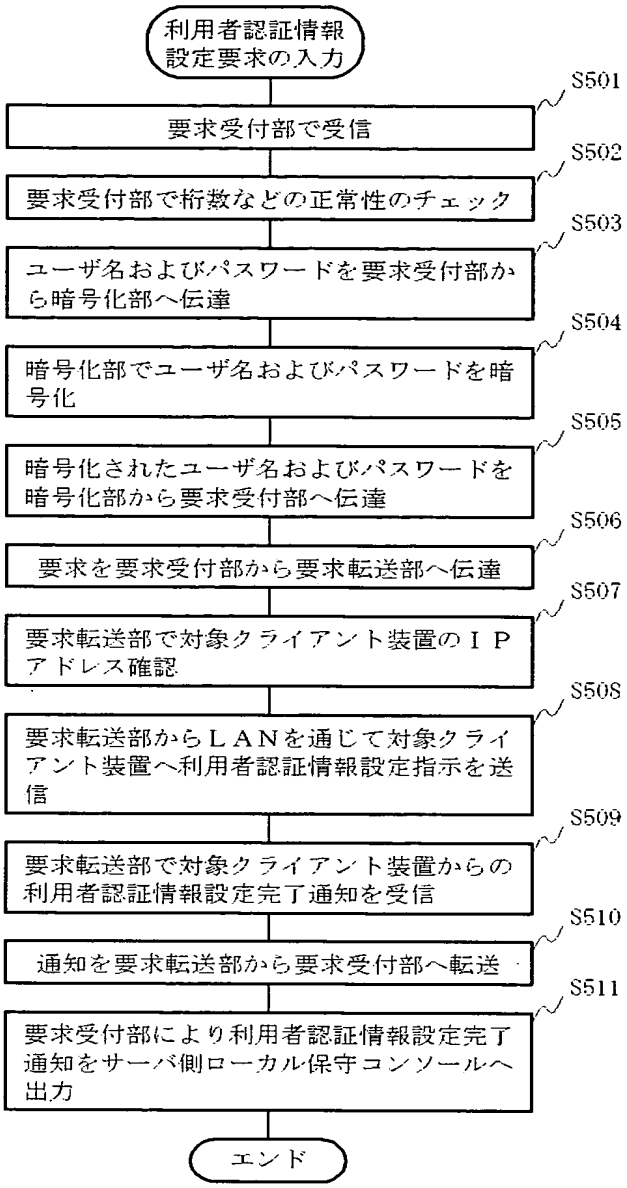
【図２０】

【図２０】


6 LAN
1
サーバ装置
暗号化部
13
11
12
要求受付部
要求転送部
2
ローカル保守
コンソール
5
遠隔保守
コンソール
3
クライアント装置
36
復号化部
33
リモート要求
処理部
38
利用時間
管理部
30
32
利用者認証部
保守インタフェース
37
強制切断部
31
35
ログイン・ログ
アウト処理部
保守対象部
3
クライアント装置
3
クライアント装置

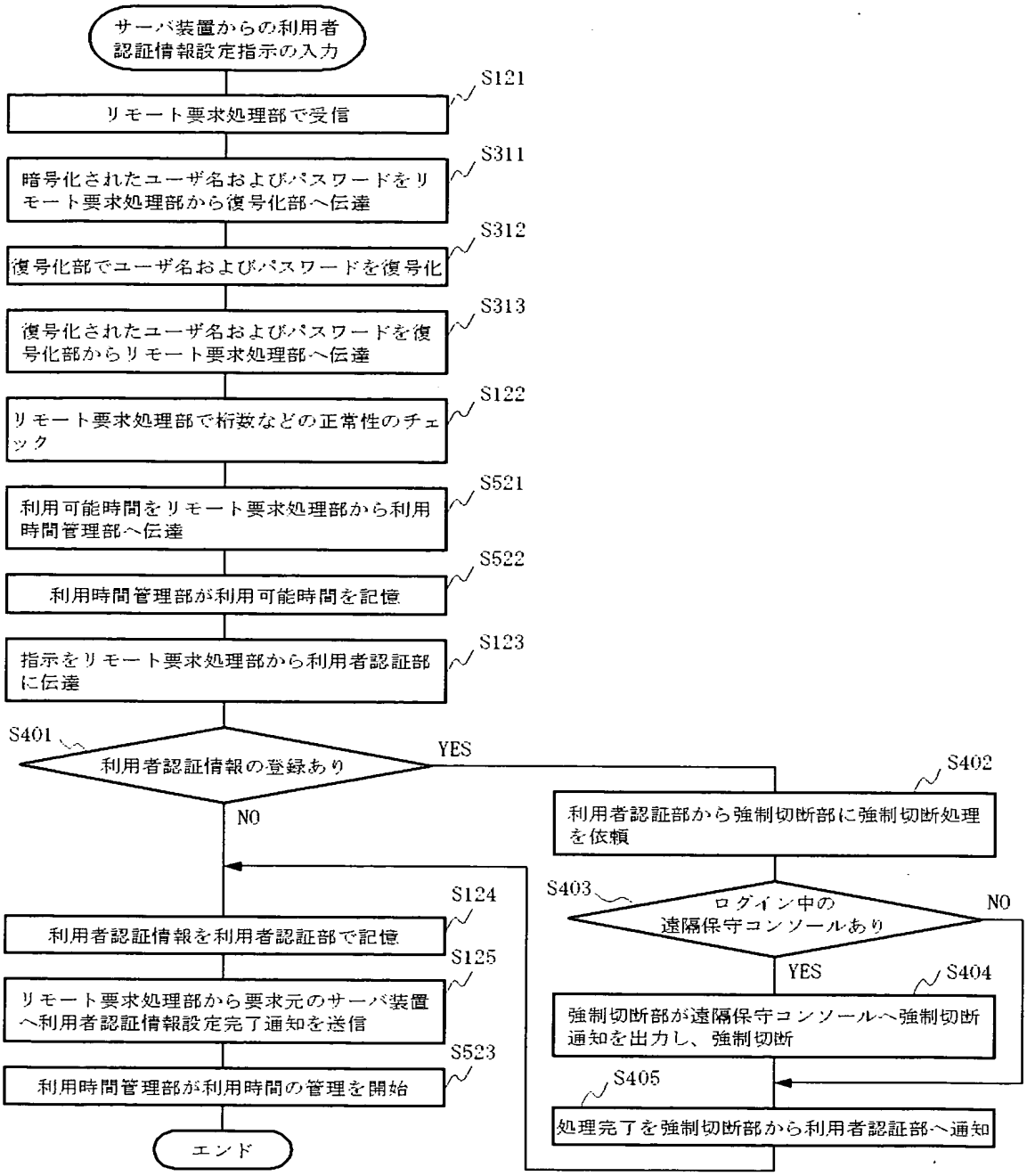
【図２１】

【図２１】


利用者認証情報設定要求の入力
S501
要求受付部で受信
S502
要求受付部で桁数などの正常性のチェック
S503
ユーザ名およびパスワードを要求受付部から暗号化部へ伝達
S504
暗号化部でユーザ名およびパスワードを暗号化
S505
暗号化されたユーザ名およびパスワードを暗号化部から要求受付部へ伝達
S506
要求を要求受付部から要求転送部へ伝達
S507
要求転送部で対象クライアント装置のＩＰアドレス確認
S508
要求転送部からＬＡＮを通じて対象クライアント装置へ利用者認証情報設定指示を送信
S509
要求転送部で対象クライアント装置からの利用者認証情報設定完了通知を受信
S510
通知を要求転送部から要求受付部へ転送
S511
要求受付部により利用者認証情報設定完了通知をサーバ側ローカル保守コンソールへ出力
エンド

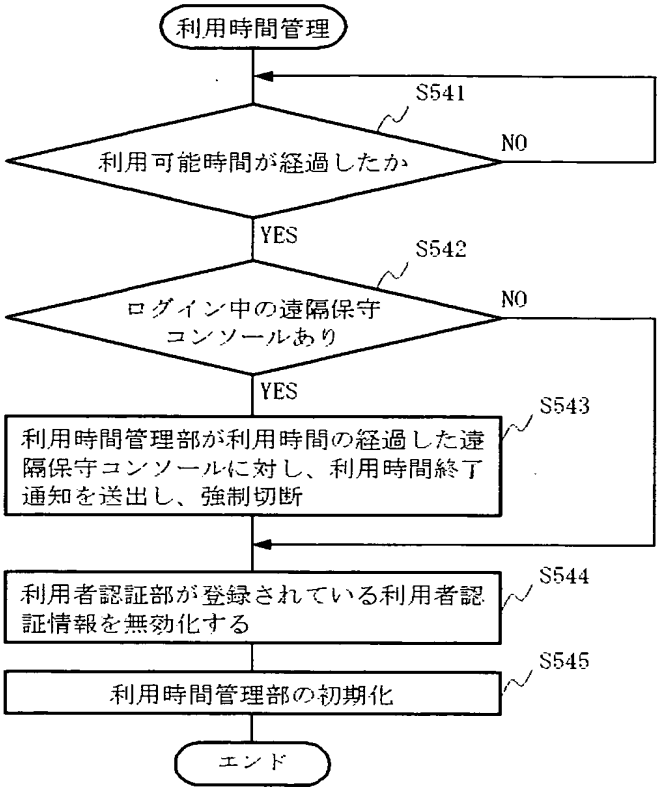
【図２２】

【図２２】


サーバ装置からの利用者認証情報設定指示の入力
S121
リモート要求処理部で受信
S311
暗号化されたユーザ名およびパスワードをリモート要求処理部から復号化部へ伝達
S312
復号化部でユーザ名およびパスワードを復号化
S313
復号化されたユーザ名およびパスワードを復号化部からリモート要求処理部へ伝達
S122
リモート要求処理部で桁数などの正常性のチェック
S521
利用可能時間をリモート要求処理部から利用時間管理部へ伝達
S522
利用時間管理部が利用可能時間を記憶
S123
指示をリモート要求処理部から利用者認証部に伝達
S401
利用者認証情報の登録あり
YES
NO
S402
利用者認証部から強制切断部に強制切断処理を依頼
S403
ログイン中の遠隔保守コンソールあり
NO
YES
S404
強制切断部が遠隔保守コンソールへ強制切断通知を出力し、強制切断
S405
処理完了を強制切断部から利用者認証部へ通知
S124
利用者認証情報を利用者認証部で記憶
S125
リモート要求処理部から要求元のサーバ装置へ利用者認証情報設定完了通知を送信
S523
利用時間管理部が利用時間の管理を開始
エンド

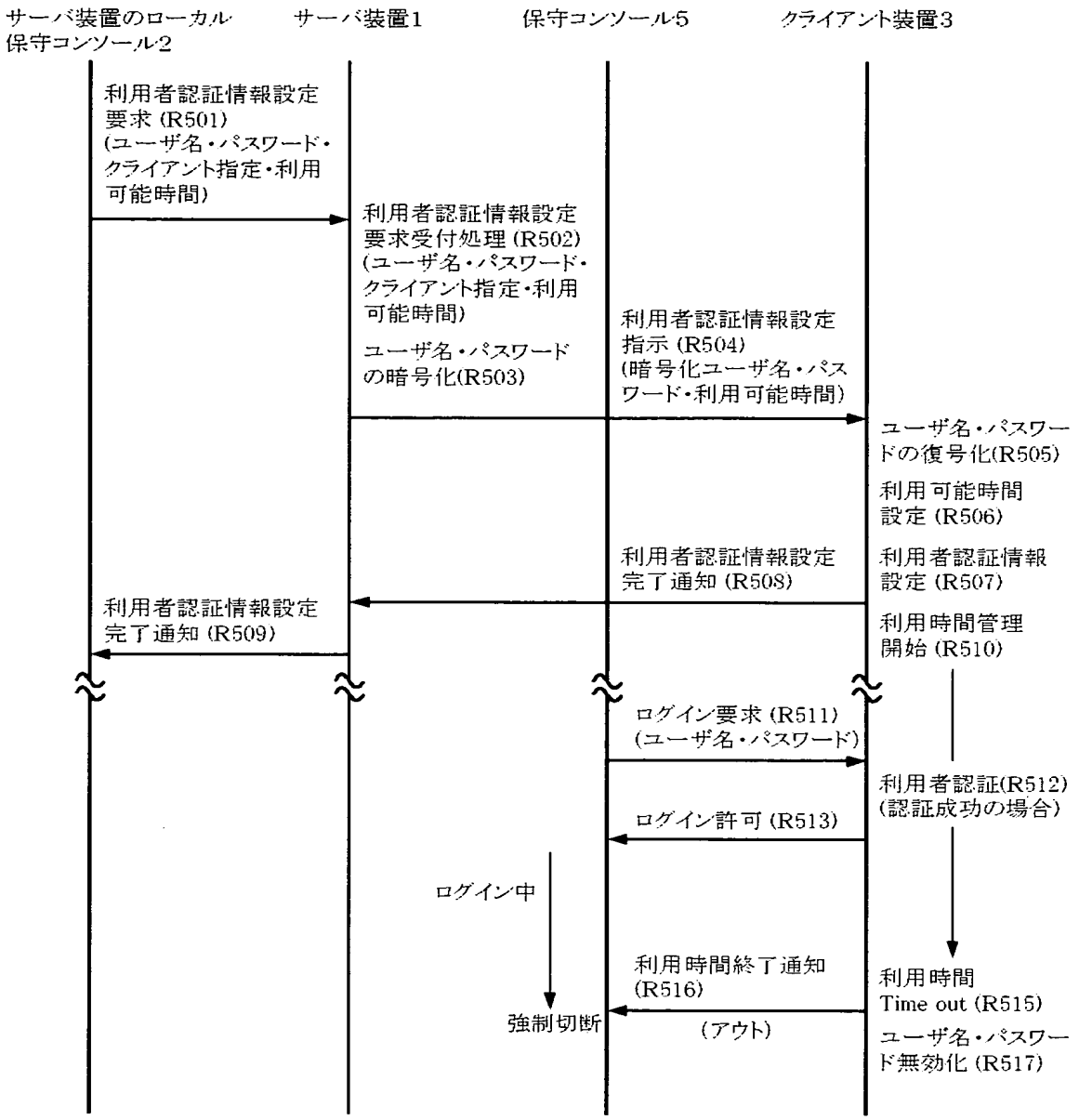
【図２３】

【図２３】


利用時間管理
S541
利用可能時間が経過したか
NO
YES
S542
ログイン中の遠隔保守コンソールあり
NO
YES
S543
利用時間管理部が利用時間の経過した遠隔保守コンソールに対し、利用時間終了通知を送出し、強制切断
S544
利用者認証部が登録されている利用者認証情報を無効化する
S545
利用時間管理部の初期化
エンド

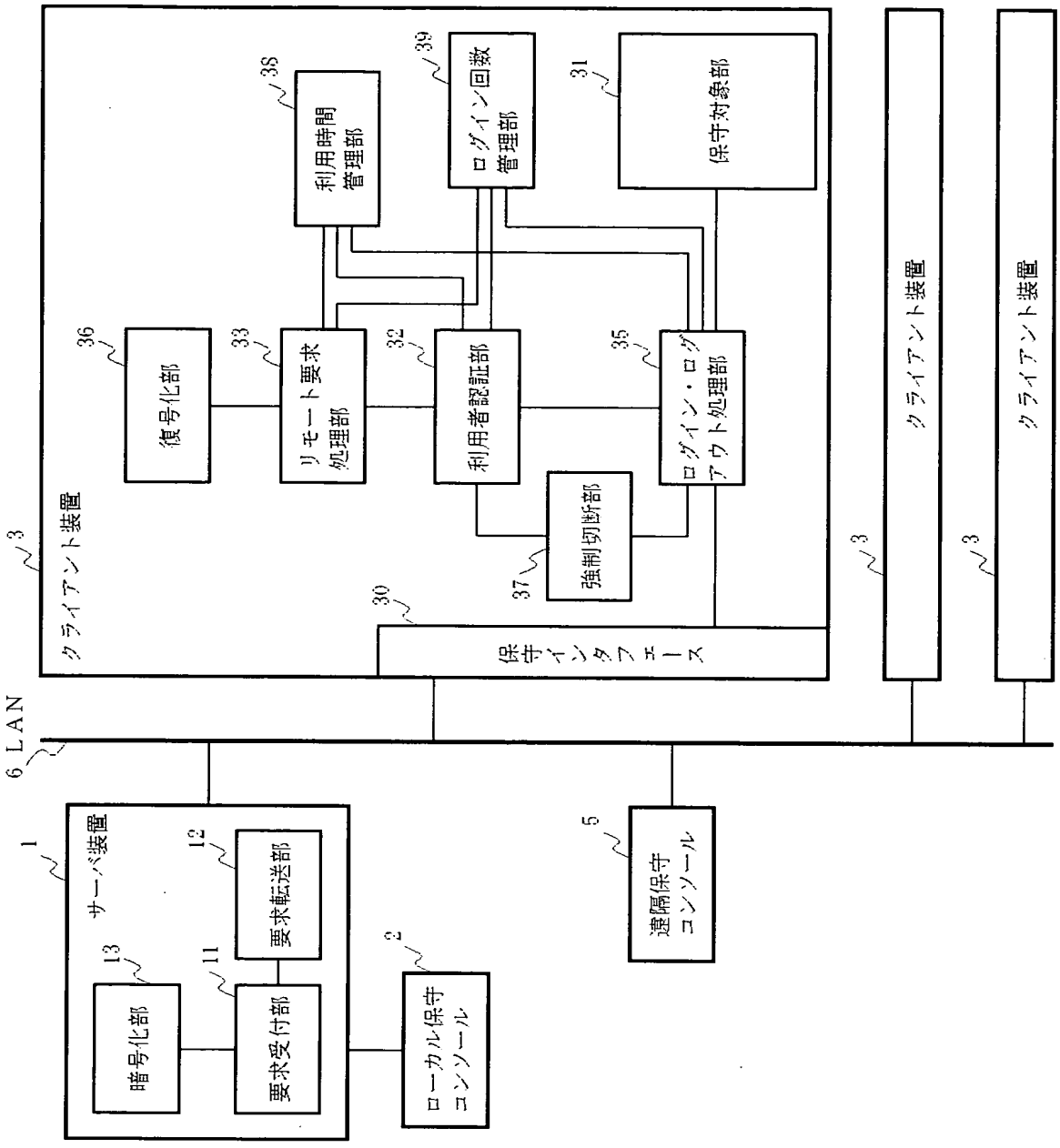
【図２４】

【図２４】


サーバ装置のローカル保守コンソール2
サーバ装置1
保守コンソール5
クライアント装置3
利用者認証情報設定要求 (R501)
(ユーザ名・パスワード・クライアント指定・利用可能時間)
利用者認証情報設定要求受付処理 (R502)
(ユーザ名・パスワード・クライアント指定・利用可能時間)
ユーザ名・パスワードの暗号化(R503)
利用者認証情報設定指示 (R504)
(暗号化ユーザ名・パスワード・利用可能時間)
ユーザ名・パスワードの復号化(R505)
利用可能時間設定 (R506)
利用者認証情報設定 (R507)
利用者認証情報設定完了通知 (R508)
利用者認証情報設定完了通知 (R509)
利用時間管理開始 (R510)
ログイン要求 (R511)
(ユーザ名・パスワード)
利用者認証(R512)
(認証成功の場合)
ログイン許可 (R513)
ログイン中
利用時間終了通知 (R516)
利用時間Time out (R515)
強制切断
(アウト)
ユーザ名・パスワード無効化 (R517)

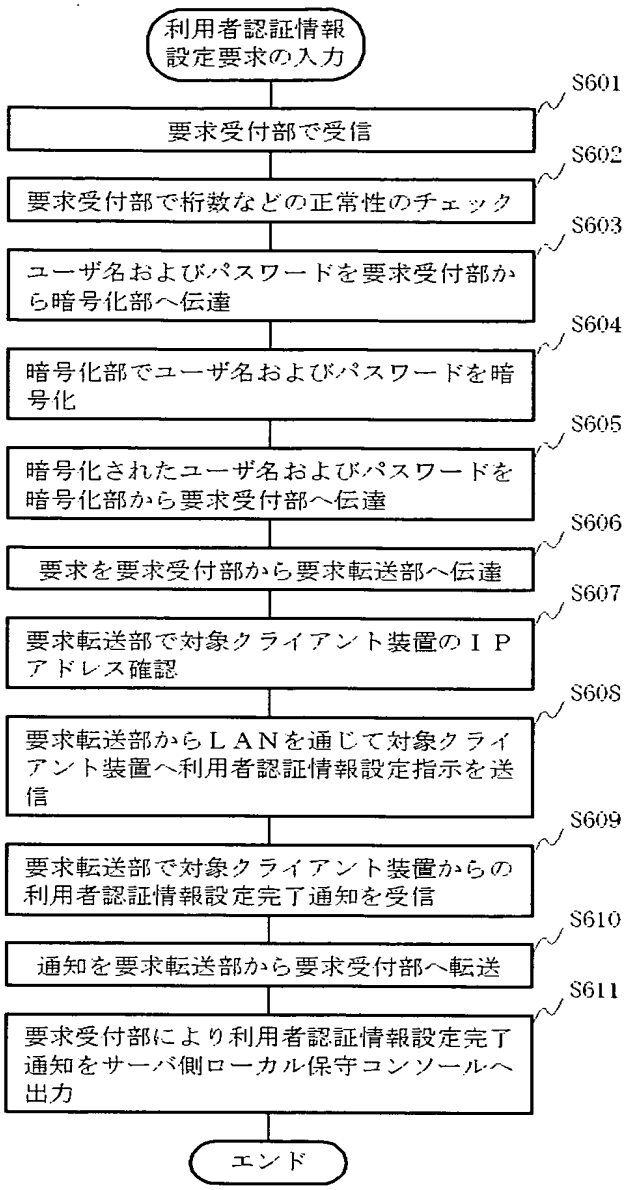
【図２５】

【図２５】


サーバ装置
1
暗号化部
13
要求受付部
11
要求転送部
12
ローカル保守コンソール
2
遠隔保守コンソール
5
6 LAN
クライアント装置
3
保守インタフェース
30
利用者認証部
32
リモート要求処理部
33
復号化部
36
利用時間管理部
38
ログイン回数管理部
39
保守対象部
31
ログイン・ログアウト処理部
35
強制切断部
37
クライアント装置
3
クライアント装置
3

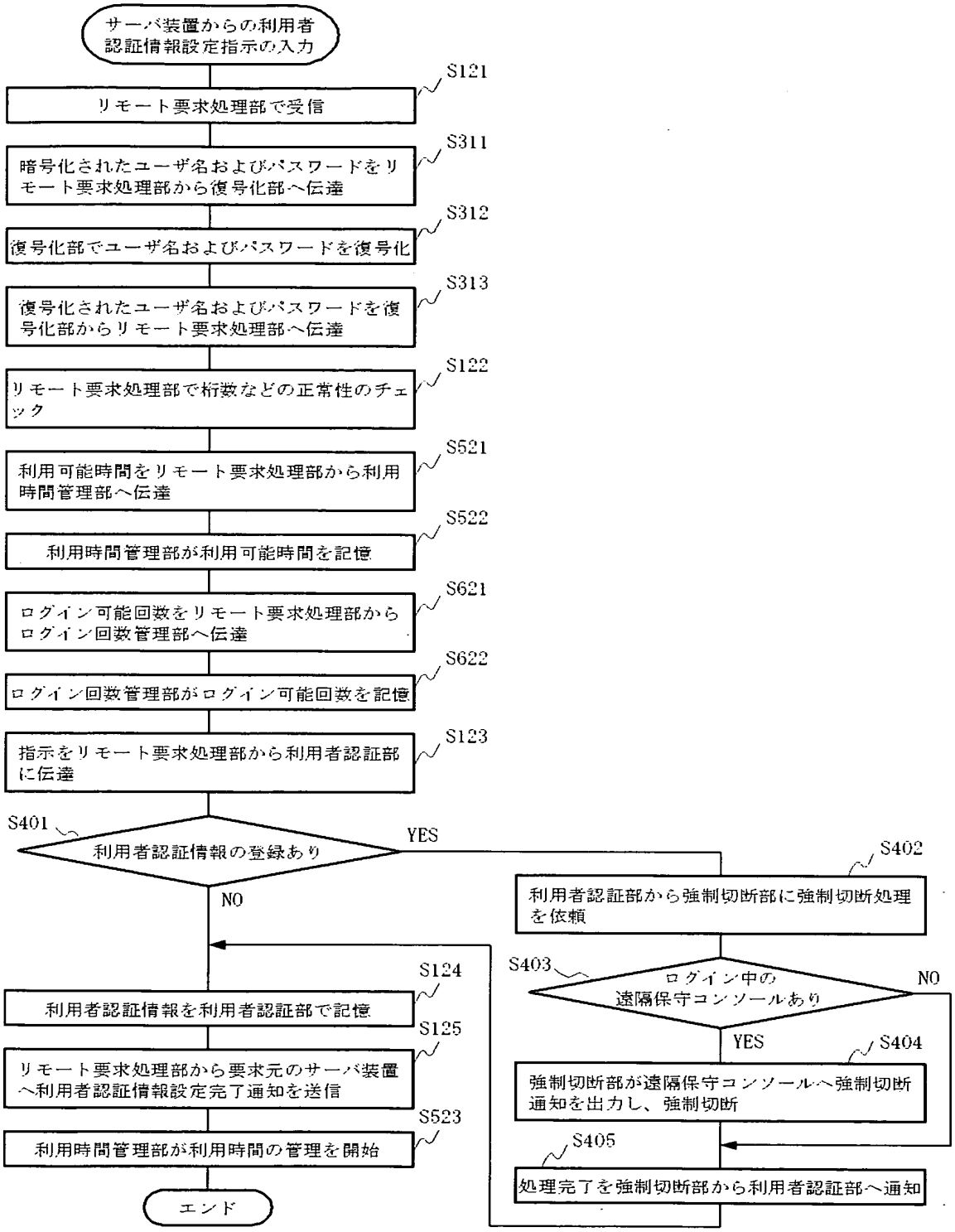
【図２６】

【図２６】


利用者認証情報設定要求の入力
S601
要求受付部で受信
S602
要求受付部で桁数などの正常性のチェック
S603
ユーザ名およびパスワードを要求受付部から暗号化部へ伝達
S604
暗号化部でユーザ名およびパスワードを暗号化
S605
暗号化されたユーザ名およびパスワードを暗号化部から要求受付部へ伝達
S606
要求を要求受付部から要求転送部へ伝達
S607
要求転送部で対象クライアント装置のＩＰアドレス確認
S608
要求転送部からＬＡＮを通じて対象クライアント装置へ利用者認証情報設定指示を送信
S609
要求転送部で対象クライアント装置からの利用者認証情報設定完了通知を受信
S610
通知を要求転送部から要求受付部へ転送
S611
要求受付部により利用者認証情報設定完了通知をサーバ側ローカル保守コンソールへ出力
エンド

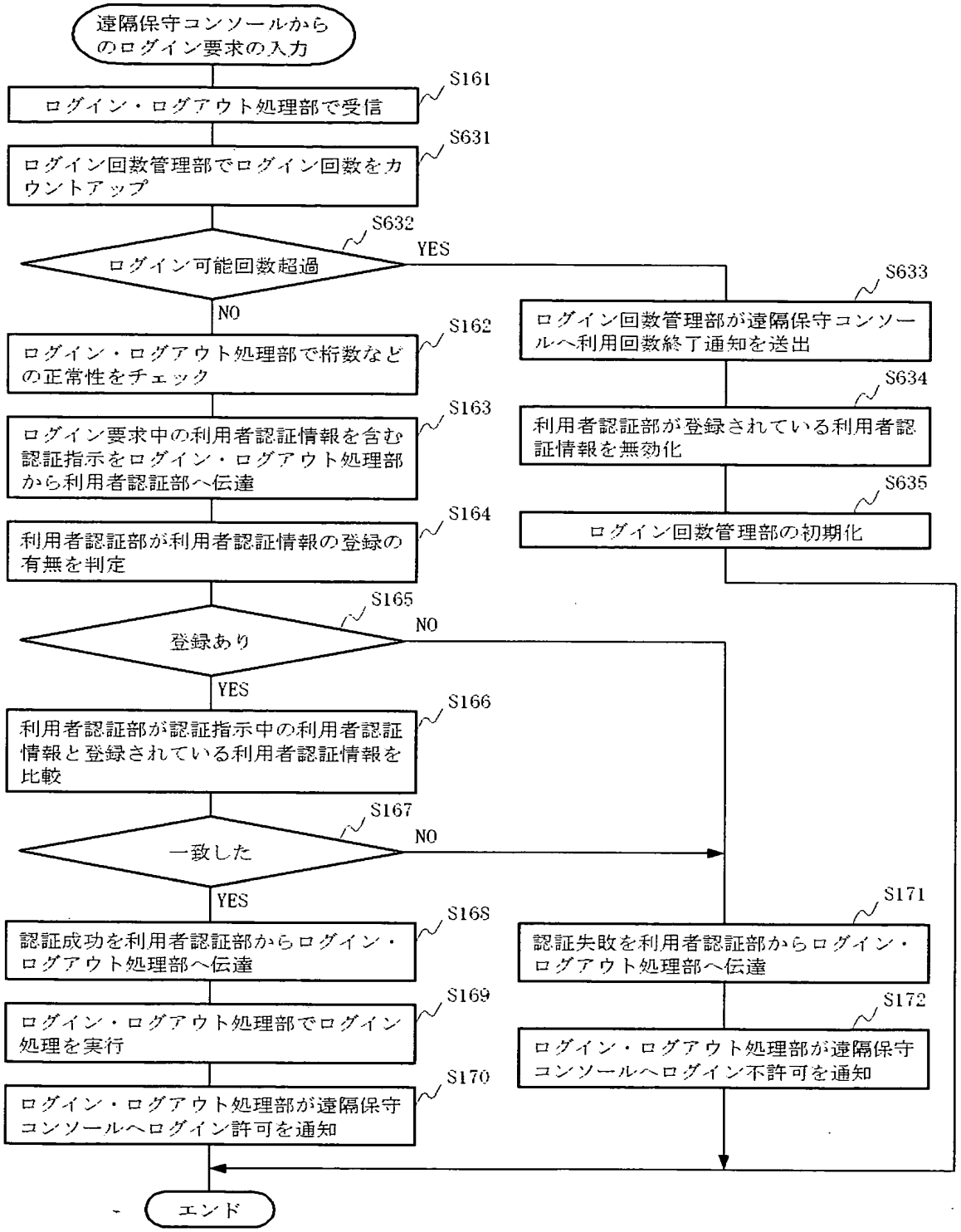
【図２７】

【図２７】


サーバ装置からの利用者認証情報設定指示の入力
S121
リモート要求処理部で受信
S311
暗号化されたユーザ名およびパスワードをリモート要求処理部から復号化部へ伝達
S312
復号化部でユーザ名およびパスワードを復号化
S313
復号化されたユーザ名およびパスワードを復号化部からリモート要求処理部へ伝達
S122
リモート要求処理部で桁数などの正常性のチェック
S521
利用可能時間をリモート要求処理部から利用時間管理部へ伝達
S522
利用時間管理部が利用可能時間を記憶
S621
ログイン可能回数をリモート要求処理部からログイン回数管理部へ伝達
S622
ログイン回数管理部がログイン可能回数を記憶
S123
指示をリモート要求処理部から利用者認証部に伝達
S401
利用者認証情報の登録あり
YES
NO
S402
利用者認証部から強制切断部に強制切断処理を依頼
S403
ログイン中の遠隔保守コンソールあり
NO
YES
S404
強制切断部が遠隔保守コンソールへ強制切断通知を出力し、強制切断
S405
処理完了を強制切断部から利用者認証部へ通知
S124
利用者認証情報を利用者認証部で記憶
S125
リモート要求処理部から要求元のサーバ装置へ利用者認証情報設定完了通知を送信
S523
利用時間管理部が利用時間の管理を開始
エンド

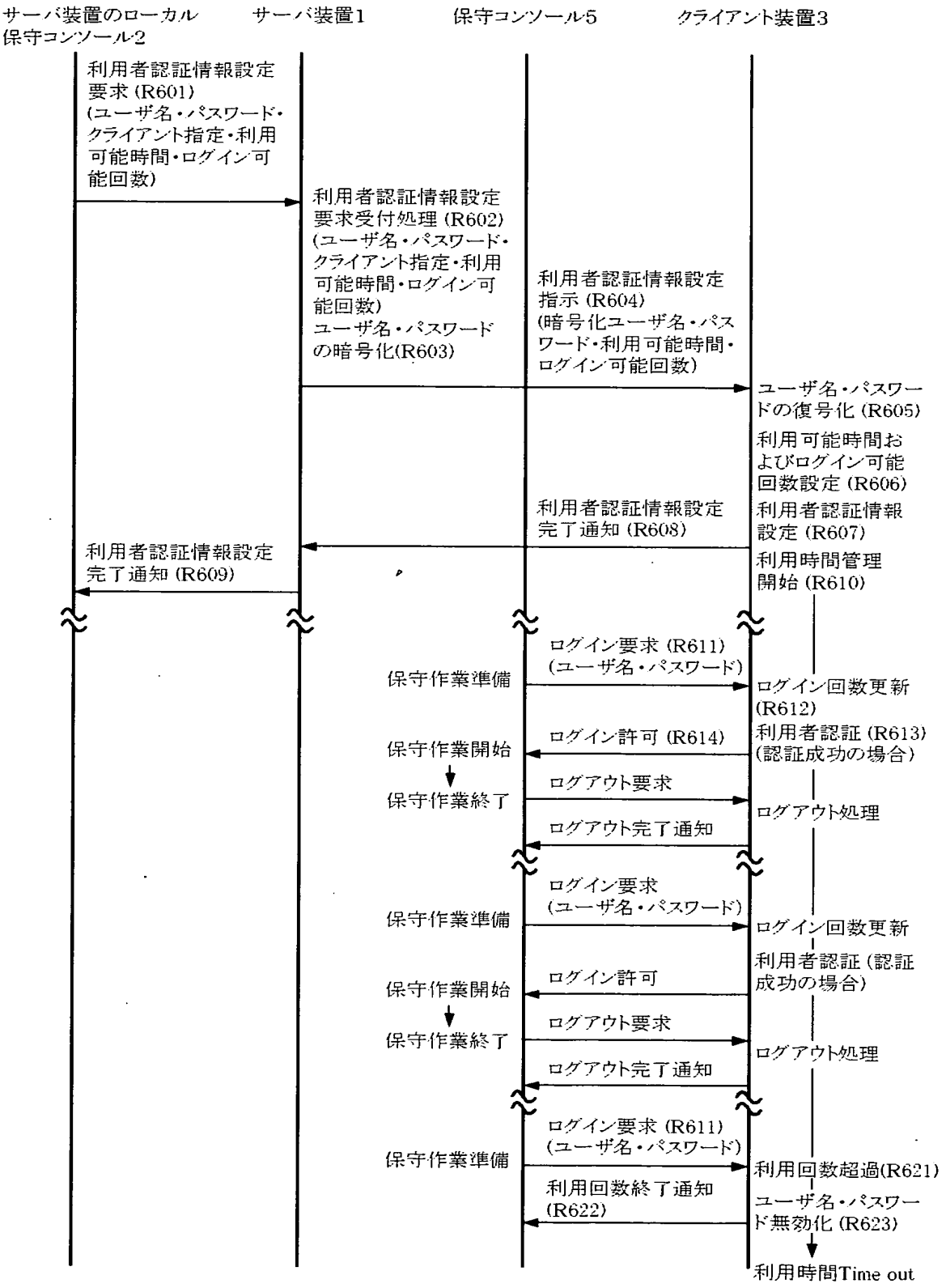
【図２８】

【図２８】


遠隔保守コンソールからのログイン要求の入力
S161
ログイン・ログアウト処理部で受信
S631
ログイン回数管理部でログイン回数をカウントアップ
S632
ログイン可能回数超過
YES
NO
S633
ログイン回数管理部が遠隔保守コンソールへ利用回数終了通知を送出
S634
利用者認証部が登録されている利用者認証情報を無効化
S635
ログイン回数管理部の初期化
S162
ログイン・ログアウト処理部で桁数などの正常性をチェック
S163
ログイン要求中の利用者認証情報を含む認証指示をログイン・ログアウト処理部から利用者認証部へ伝達
S164
利用者認証部が利用者認証情報の登録の有無を判定
S165
登録あり
NO
YES
S166
利用者認証部が認証指示中の利用者認証情報と登録されている利用者認証情報を比較
S167
一致した
NO
YES
S168
認証成功を利用者認証部からログイン・ログアウト処理部へ伝達
S169
ログイン・ログアウト処理部でログイン処理を実行
S170
ログイン・ログアウト処理部が遠隔保守コンソールへログイン許可を通知
S171
認証失敗を利用者認証部からログイン・ログアウト処理部へ伝達
S172
ログイン・ログアウト処理部が遠隔保守コンソールへログイン不許可を通知
エンド

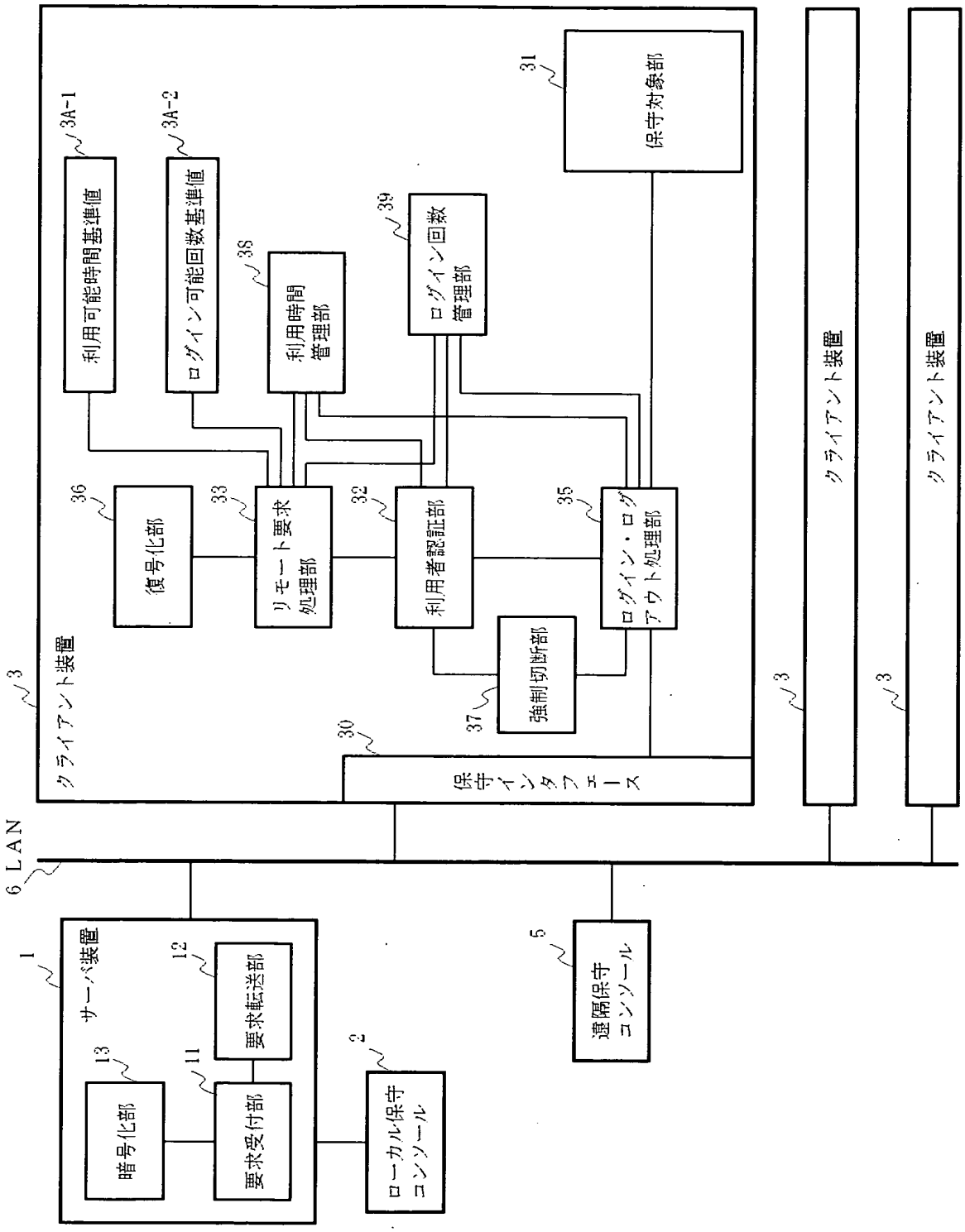
【図２９】

【図２９】


サーバ装置のローカル保守コンソール2
サーバ装置1
保守コンソール5
クライアント装置3
利用者認証情報設定要求 (R601)
(ユーザ名・パスワード・クライアント指定・利用可能時間・ログイン可能回数)
利用者認証情報設定要求受付処理 (R602)
(ユーザ名・パスワード・クライアント指定・利用可能時間・ログイン可能回数)
ユーザ名・パスワードの暗号化(R603)
利用者認証情報設定指示 (R604)
(暗号化ユーザ名・パスワード・利用可能時間・ログイン可能回数)
ユーザ名・パスワードの復号化 (R605)
利用可能時間およびログイン可能回数設定 (R606)
利用者認証情報設定 (R607)
利用者認証情報設定完了通知 (R608)
利用者認証情報設定完了通知 (R609)
利用時間管理開始 (R610)
ログイン要求 (R611)
(ユーザ名・パスワード)
保守作業準備
ログイン回数更新 (R612)
利用者認証 (R613)
(認証成功の場合)
ログイン許可 (R614)
保守作業開始
保守作業終了
ログアウト要求
ログアウト処理
ログアウト完了通知
ログイン要求
(ユーザ名・パスワード)
保守作業準備
ログイン回数更新
利用者認証 (認証成功の場合)
ログイン許可
保守作業開始
保守作業終了
ログアウト要求
ログアウト処理
ログアウト完了通知
ログイン要求 (R611)
(ユーザ名・パスワード)
保守作業準備
利用回数超過(R621)
利用回数終了通知 (R622)
ユーザ名・パスワード無効化 (R623)
利用時間Time out

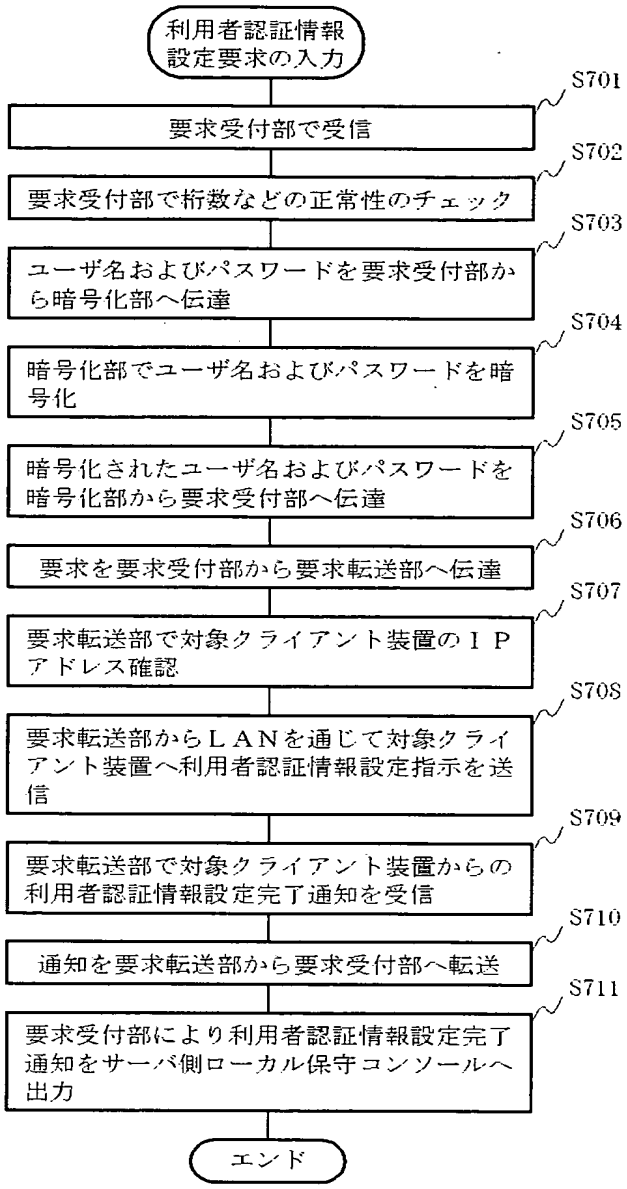
【図３０】

【図３０】


1
サーバ装置
暗号化部
13
要求受付部
11
要求転送部
12
2
ローカル保守コンソール
6 LAN
5
遠隔保守コンソール
3
クライアント装置
保守インタフェース
30
強制切断部
37
利用者認証部
32
ログイン・ログアウト処理部
35
リモート要求処理部
33
復号化部
36
利用時間管理部
38
ログイン回数管理部
39
ログイン可能回数基準値
3A-2
利用可能時間基準値
3A-1
保守対象部
31
クライアント装置
3
クライアント装置
3

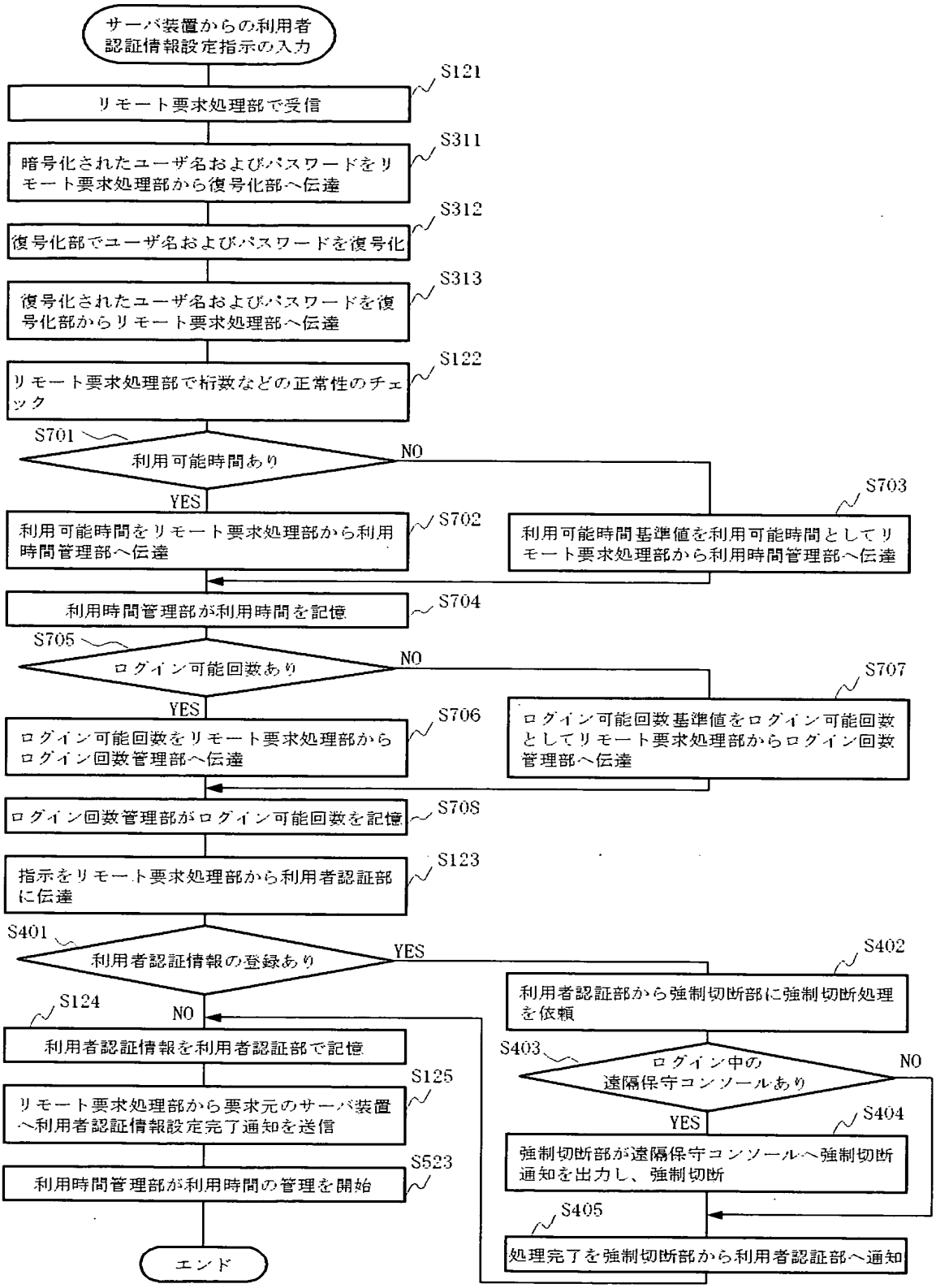
【図３１】

【図３１】


利用者認証情報設定要求の入力
S701
要求受付部で受信
S702
要求受付部で桁数などの正常性のチェック
S703
ユーザ名およびパスワードを要求受付部から暗号化部へ伝達
S704
暗号化部でユーザ名およびパスワードを暗号化
S705
暗号化されたユーザ名およびパスワードを暗号化部から要求受付部へ伝達
S706
要求を要求受付部から要求転送部へ伝達
S707
要求転送部で対象クライアント装置のＩＰアドレス確認
S708
要求転送部からＬＡＮを通じて対象クライアント装置へ利用者認証情報設定指示を送信
S709
要求転送部で対象クライアント装置からの利用者認証情報設定完了通知を受信
S710
通知を要求転送部から要求受付部へ転送
S711
要求受付部により利用者認証情報設定完了通知をサーバ側ローカル保守コンソールへ出力
エンド

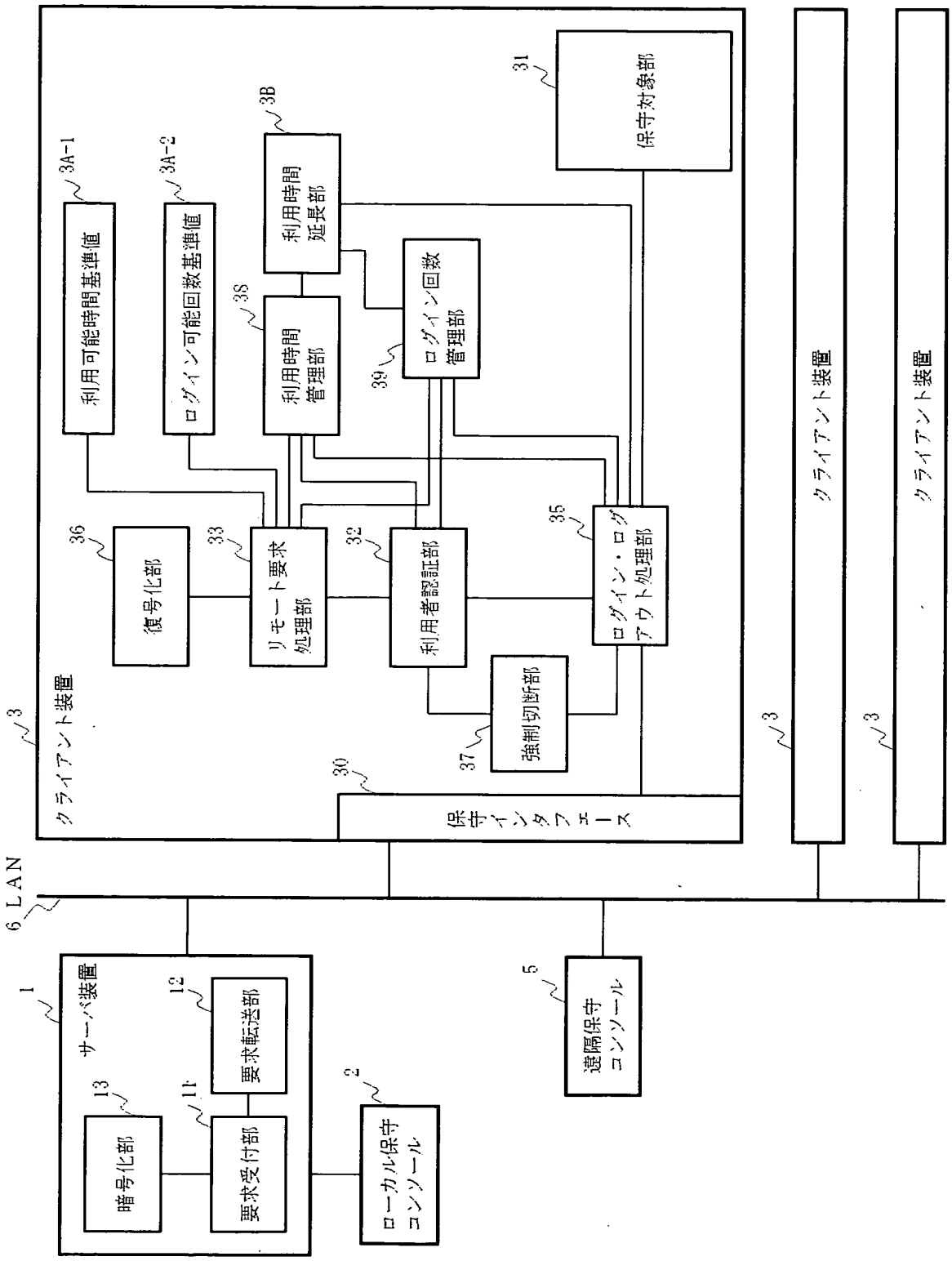
【図３２】

【図３２】


サーバ装置からの利用者認証情報設定指示の入力
S121
リモート要求処理部で受信
S311
暗号化されたユーザ名およびパスワードをリモート要求処理部から復号化部へ伝達
S312
復号化部でユーザ名およびパスワードを復号化
S313
復号化されたユーザ名およびパスワードを復号化部からリモート要求処理部へ伝達
S122
リモート要求処理部で桁数などの正常性のチェック
S701
利用可能時間あり
NO
YES
S703
利用可能時間基準値を利用可能時間としてリモート要求処理部から利用時間管理部へ伝達
S702
利用可能時間をリモート要求処理部から利用時間管理部へ伝達
S704
利用時間管理部が利用時間を記憶
S705
ログイン可能回数あり
NO
YES
S707
ログイン可能回数基準値をログイン可能回数としてリモート要求処理部からログイン回数管理部へ伝達
S706
ログイン可能回数をリモート要求処理部からログイン回数管理部へ伝達
S708
ログイン回数管理部がログイン可能回数を記憶
S123
指示をリモート要求処理部から利用者認証部に伝達
S401
利用者認証情報の登録あり
YES
NO
S402
利用者認証部から強制切断部に強制切断処理を依頼
S124
利用者認証情報を利用者認証部で記憶
S403
ログイン中の遠隔保守コンソールあり
NO
YES
S125
リモート要求処理部から要求元のサーバ装置へ利用者認証情報設定完了通知を送信
S404
強制切断部が遠隔保守コンソールへ強制切断通知を出力し、強制切断
S523
利用時間管理部が利用時間の管理を開始
S405
処理完了を強制切断部から利用者認証部へ通知
エンド

【図３３】

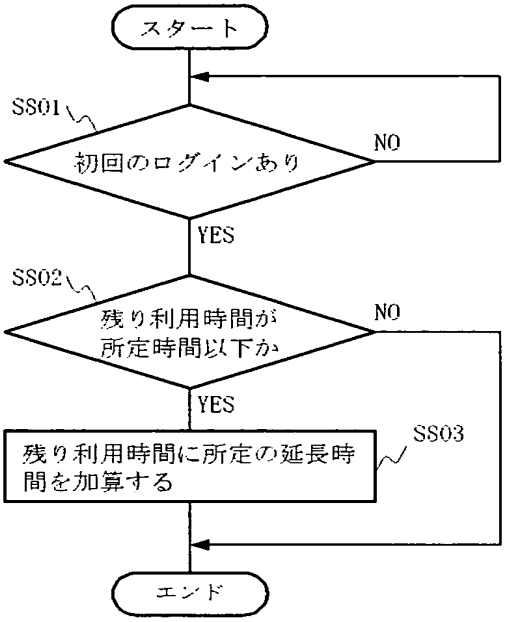
【図３３】


サーバ装置
1
暗号化部
13
要求受付部
11
要求転送部
12
ローカル保守コンソール
2
6 LAN
遠隔保守コンソール
5
クライアント装置
3
クライアント装置
3
クライアント装置
3
保守インタフェース
30
利用可能時間基準値
3A-1
ログイン可能回数基準値
3A-2
利用時間延長部
3B
保守対象部
31
利用時間管理部
38
ログイン回数管理部
39
復号化部
36
リモート要求処理部
33
利用者認証部
32
ログイン・ログアウト処理部
35
強制切断部
37

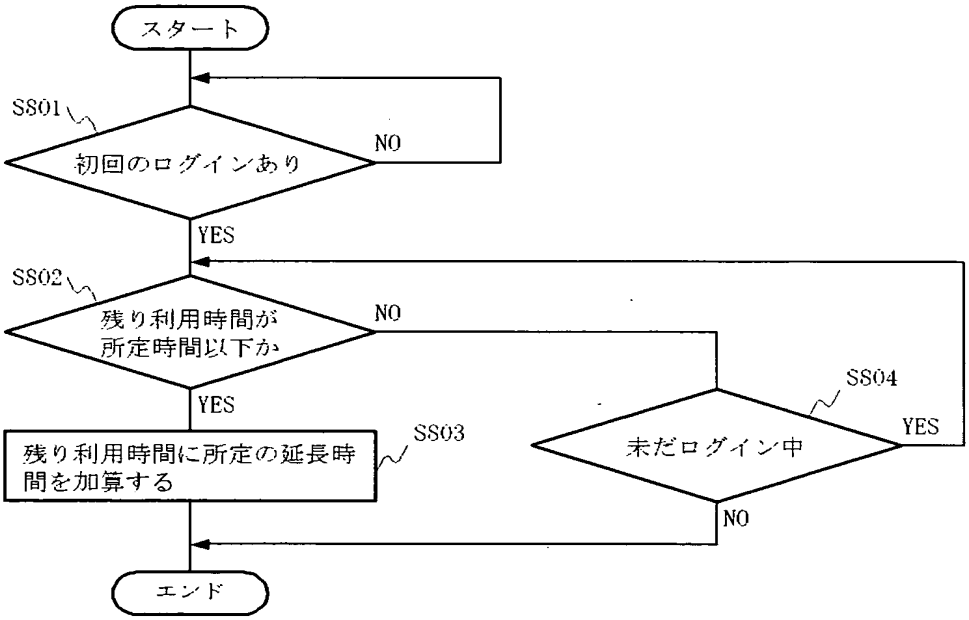
【図３４】

【図３４】

(A)

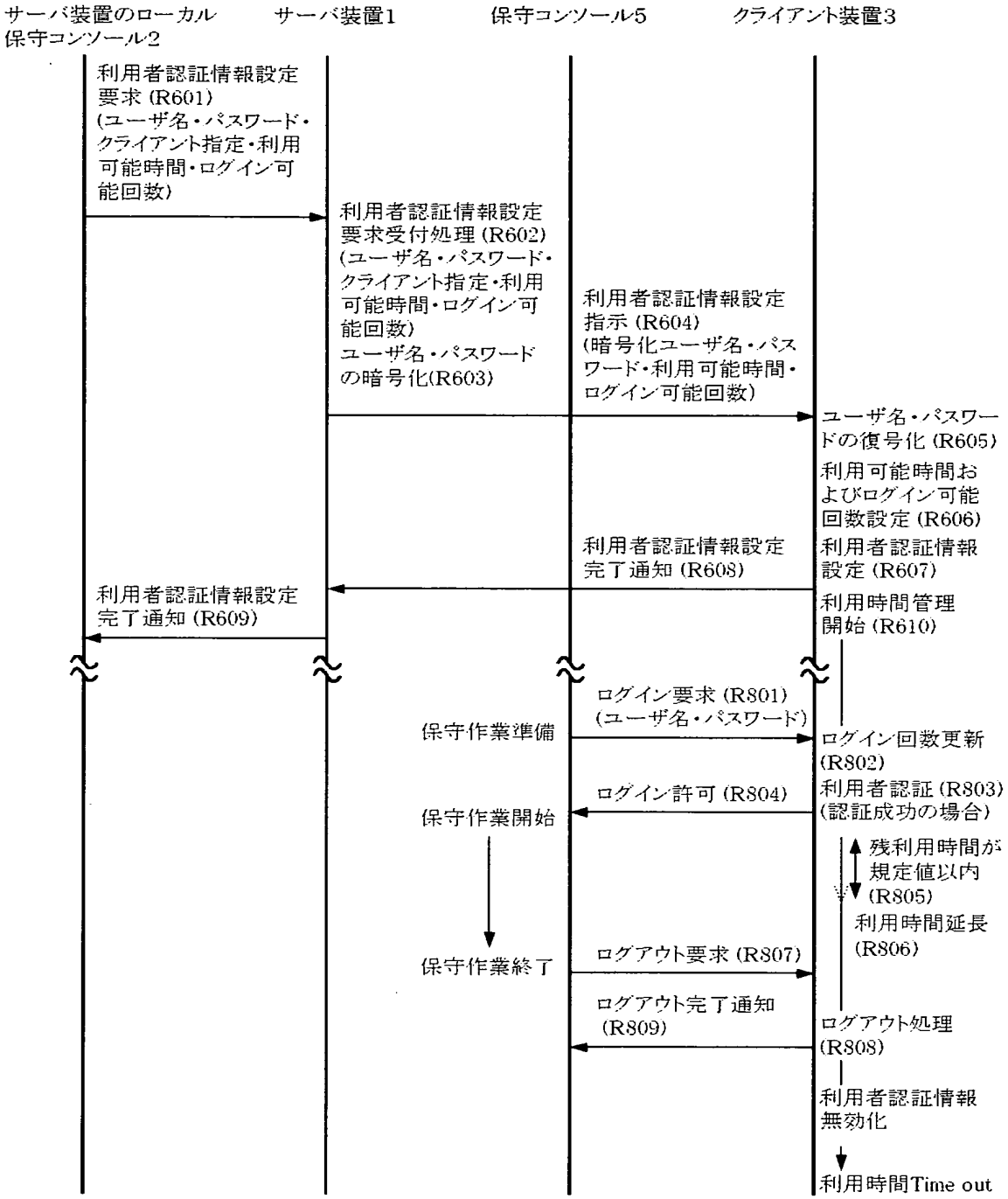

スタート
SS01
初回のログインあり
NO
YES
SS02
残り利用時間が
所定時間以下か
NO
YES
残り利用時間に所定の延長時
間を加算する
SS03
エンド

(B)


スタート
SS01
初回のログインあり
NO
YES
SS02
残り利用時間が
所定時間以下か
NO
YES
残り利用時間に所定の延長時
間を加算する
SS03
SS04
未だログイン中
YES
NO
エンド

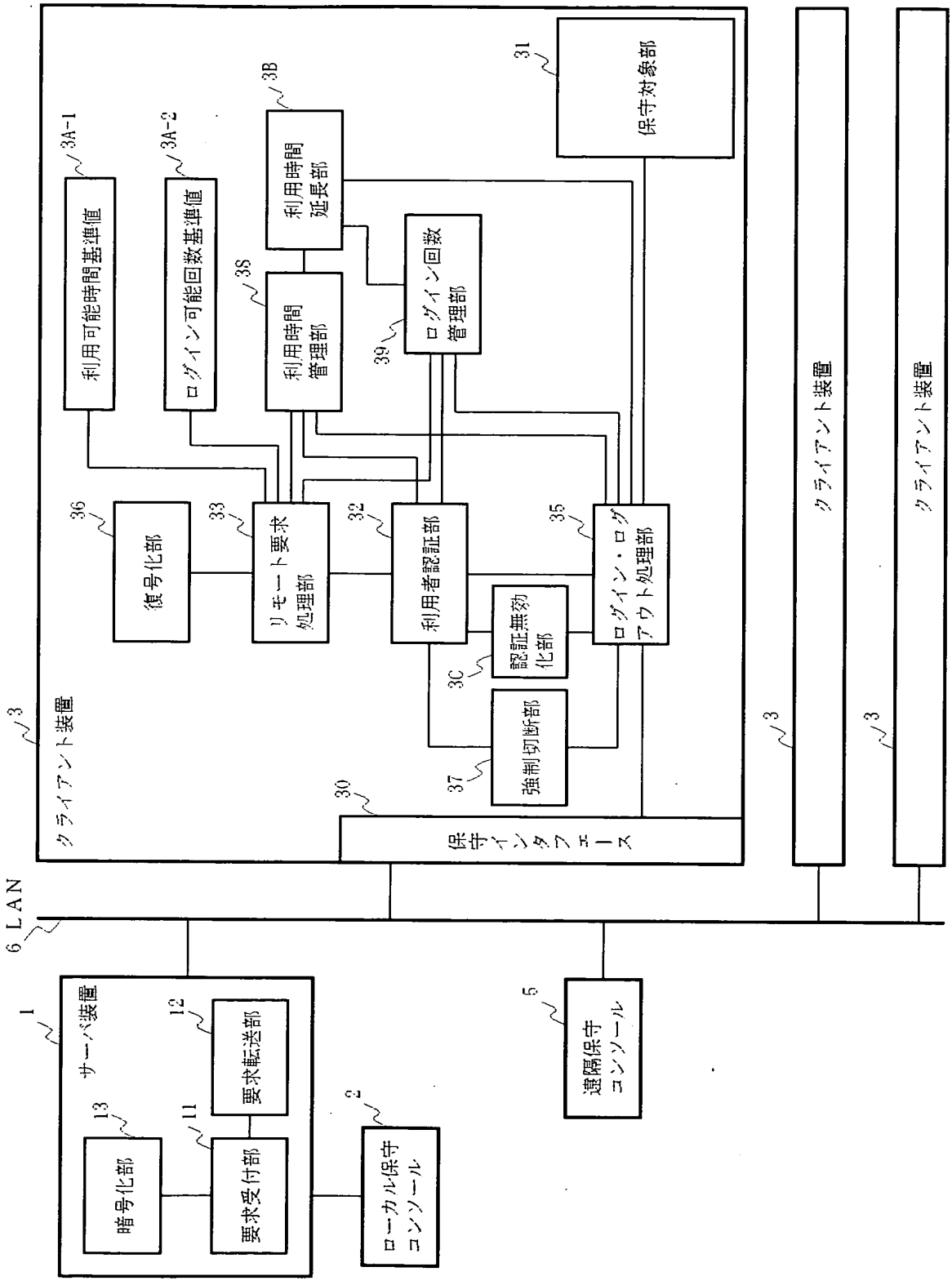
【図３５】

【図３５】


サーバ装置のローカル保守コンソール2
サーバ装置1
保守コンソール5
クライアント装置3
利用者認証情報設定要求 (R601) (ユーザ名・パスワード・クライアント指定・利用可能時間・ログイン可能回数)
利用者認証情報設定要求受付処理 (R602) (ユーザ名・パスワード・クライアント指定・利用可能時間・ログイン可能回数)
ユーザ名・パスワードの暗号化(R603)
利用者認証情報設定指示 (R604) (暗号化ユーザ名・パスワード・利用可能時間・ログイン可能回数)
ユーザ名・パスワードの復号化 (R605)
利用可能時間およびログイン可能回数設定 (R606)
利用者認証情報設定 (R607)
利用者認証情報設定完了通知 (R608)
利用者認証情報設定完了通知 (R609)
利用時間管理開始 (R610)
ログイン要求 (R801) (ユーザ名・パスワード)
保守作業準備
ログイン回数更新 (R802)
利用者認証 (R803) (認証成功の場合)
ログイン許可 (R804)
保守作業開始
残利用時間が規定値以内 (R805)
利用時間延長 (R806)
保守作業終了
ログアウト要求 (R807)
ログアウト完了通知 (R809)
ログアウト処理 (R808)
利用者認証情報無効化
利用時間Time out

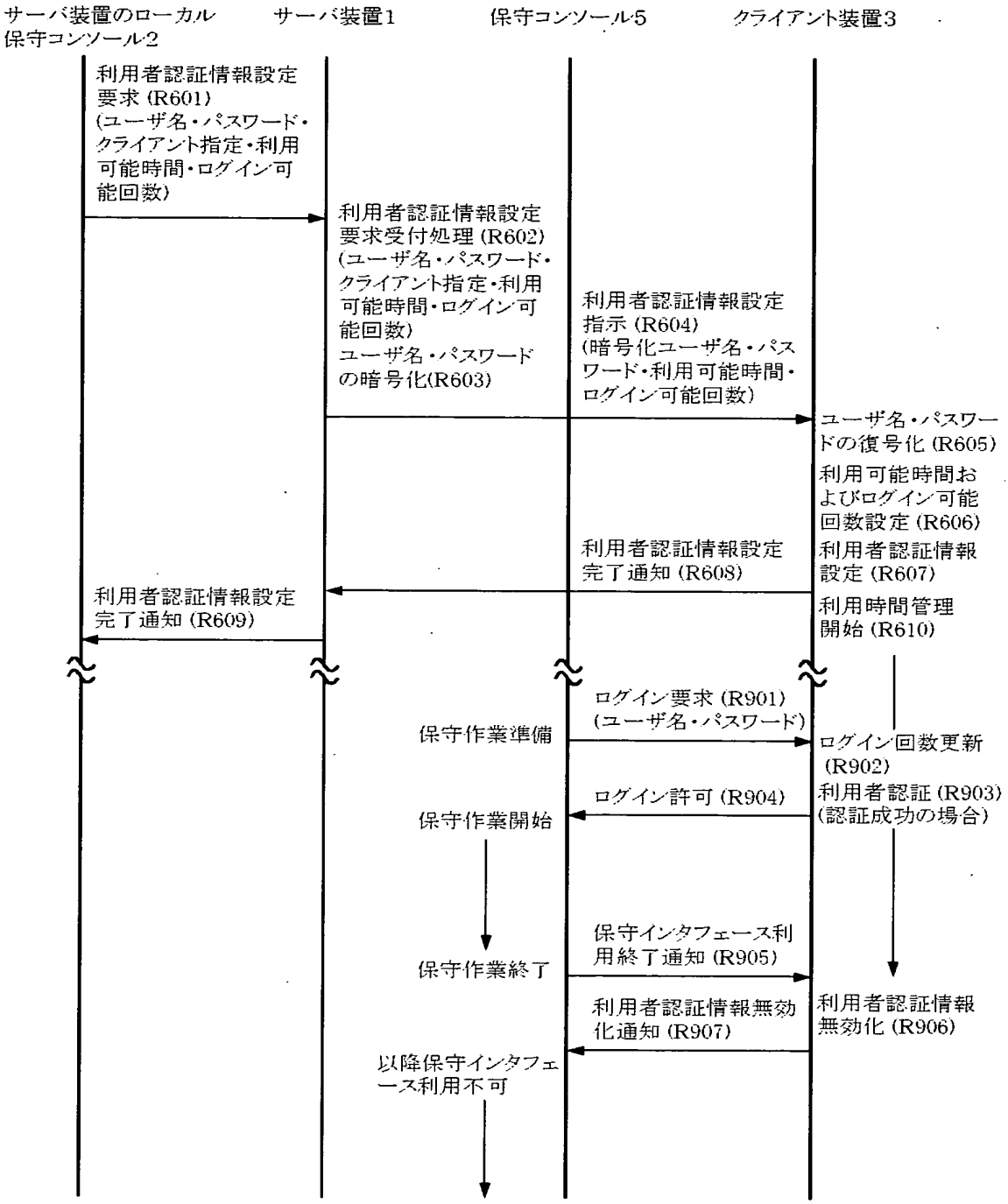
【図３６】

【図３６】


クライアント装置
3
利用可能時間基準値
3A-1
ログイン可能回数基準値
3A-2
利用時間延長部
3B
利用時間管理部
3S
ログイン回数管理部
39
保守対象部
31
復号化部
36
リモート要求処理部
33
利用者認証部
32
ログイン・ログアウト処理部
35
認証無効化部
3C
強制切断部
37
保守インタフェース
30
クライアント装置
3
クライアント装置
3
6 LAN
サーバ装置
1
暗号化部
13
要求受付部
11
要求転送部
12
ローカル保守コンソール
2
遠隔保守コンソール
5

【図３７】

【図３７】


サーバ装置のローカル保守コンソール2
サーバ装置1
保守コンソール5
クライアント装置3
利用者認証情報設定要求 (R601) (ユーザ名・パスワード・クライアント指定・利用可能時間・ログイン可能回数)
利用者認証情報設定要求受付処理 (R602) (ユーザ名・パスワード・クライアント指定・利用可能時間・ログイン可能回数)
ユーザ名・パスワードの暗号化(R603)
利用者認証情報設定指示 (R604) (暗号化ユーザ名・パスワード・利用可能時間・ログイン可能回数)
ユーザ名・パスワードの復号化 (R605)
利用可能時間およびログイン可能回数設定 (R606)
利用者認証情報設定 (R607)
利用者認証情報設定完了通知 (R608)
利用者認証情報設定完了通知 (R609)
利用時間管理開始 (R610)
ログイン要求 (R901) (ユーザ名・パスワード)
保守作業準備
ログイン回数更新 (R902)
利用者認証 (R903) (認証成功の場合)
ログイン許可 (R904)
保守作業開始
保守インタフェース利用終了通知 (R905)
保守作業終了
利用者認証情報無効化 (R906)
利用者認証情報無効化通知 (R907)
以降保守インタフェース利用不可

【書類名】　要約書

【要約】

【課題】　クライアント・サーバ型分散システムにおいて、クライアント装置の保守インタフェースの開放、閉塞をサーバ装置から遠隔で行えるようにする。

【解決の手段】　サーバ装置１の要求受付部１１は、サーバ側コンソール２から、利用者認証情報とクライアント装置３の指定とを含む報設定要求、クライアント装置３の指定を含む設定無効要求を受け付け、要求転送部１２はＬＡＮ６を通じて指定されたクライアント装置３に転送する。クライアント装置３のリモート要求処理部３３は、受信した設定要求中の利用者認証情報を、保守インタフェース３０を利用する利用者の認証を行う利用者認証部３２に設定し、保守インタフェース３０を開放する。また、設定無効要求を受信したときは、利用者認証部３２に設定されている利用者認証情報を無効にして保守インタフェース３０を閉塞する。

【選択図】　図１

特願２００２－３５６８３９

出　願　人　履　歴　情　報

識別番号　　［０００００４２３７］

１．変更年月日　　１９９０年　８月２９日
［変更理由］　　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社